
**Facebook's Misleading Data and Marketing Policies and Practices**
**Center for Digital Democracy**
**October 2013**

## I. Introduction

Facebook makes markedly different—at times completely opposite—statements to advertisers than they do to users about the type of data they make available to marketers. To users, for example, Facebook states that it will not share or "give your content or information to advertisers without your consent." In practice, however, Facebook does give advertisers user information by matching, linking, hashing, reverse engineering, and creating new IDs that are specific to individuals and persist beyond the Facebook platform. Facebook gives advertisers access to these new IDs, allowing them to follow specific individual users and tie their own external data to these IDs. This allows advertisers to expand their knowledge of specific Facebook users. By creating a parallel system of personal identification, Facebook not only shares data by matching, linking, and tying covered information but they share data that are personally identifiable.

Facebook also claims that it has instituted a system where users can opt out of this marketing and data collection. However, in practice this is an extremely convoluted and misleading process, consisting of multiple steps buried within the Facebook platform. There is no simple way for a user to opt out of this extensive data collection or targeted marketing based on tracking. A user must visit each third-party website individually to actually be informed about is data collection practices (and even then the opt-outs are cookie-based, so any clearing of browser cookies essential opts the user back into the system).

While this creation and matching of persistent personal IDs have become common data and marketing practices for Facebook, very few consumers have any level of understanding of how this process operates and its implications for privacy. The Federal Trade Commission should address the practices we discuss below, as part of its review on the proposed Data Use policy changes.

## II. Sharing User Information: Matching and Tying Covered information through the Facebook Exchange, Partner Categories, and Custom Audiences.

### Facebook's Main Advertising and Retargeting Platforms

Facebook Exchange (FBX) is Facebook's real-time bidding platform. You must be a qualified company to be a part of the exchange that currently boasts 20 approved data gathering and targeting companies. Among them are AdRoll, AppNexus, Criteo, and Media Math. FBX allows companies to follow visitors from their websites or across the

Internet back to Facebook for retargeted advertising. Custom Audiences is the mechanism by which Facebook allows marketers to reach their offline audiences among Facebook users "using email addresses, phone numbers, Facebook user IDs or app user ID's to make the match"[1]

Last April 2013, Facebook announced Partner Categories, which offers marketers a self-serve mechanism for targeting their customers.[2] It helps marketers target users based not only on their expressed interests but also on actions they have taken across the Internet regardless of device. Marketers using this platform have access to offline data from data brokerage companies Acxiom, Datalogix, and Epsilson.[3] The 500-plus unique group categories are available to marketers through Power Editor and the API.[4]

In a privacy-related post called "Advertising and our Third-Party Partners," Facebook describes its new relationship with leading data broker companies as "partnerships [designed] with people's privacy in mind and how people using Facebook continue to have control over the ads they see."[5] The blog explains that Facebook's work with Acxiom, for example, is innocuous, beneficial, and reflects current business practices used by others: "Many businesses today work with third parties such as Acxiom, Datalogix, and Epsilon to help manage and understand their marketing efforts. For example, an auto dealer may want to customize an offer to people who are likely to be in the market for a new car. The dealer also might want to send offers, like discounts for service, to customers that have purchased a car from them. To do this, the auto dealer works with a third-party company to identify and reach those customers with the right offer."[6]

On a page discussing "Third-party service providers" Facebook states that "[w]e may work with others to combine information we have collected from you with info provided by an advertiser, to enable the advertiser to send you relevant advertising."[7] In a page for marketers, Facebook explains the service differently:

---

[1] https://www.facebook.com/help/341425252616329; http://www.facebook-pmdcenter.com/fbx

[2] https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature

[3] https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature; http://www.facebook-pmdcenter.com/fbx; http://blog.adespresso.com/facebook-partner-categories-guide/

[4] https://www.facebook.com/help/194355723944655/

[5] https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729

[6] https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729

[7] https://www.facebook.com/notes/facebook-and-privacy/targeting-and-our-third-party-partners/532721576777729; https://www.facebook.com/help/133547810119620

> To date, advertisers have been able to show ads to people based on their expressed interests on Facebook. Now with partner categories, they can also show ads to people on Facebook based on the products and brands they buy across both desktop and mobile,
>
> Partner categories uses data from select third parties including Acxiom, Datalogix, and Epsilon. No personal information is shared between Facebook, third parties or advertisers. Partner categories work the same way all targeting on Facebook works. The advertiser only knows the size of the audience and can't access any information about individuals included in a category.[8]

Facebook explains Partner Categories to its ad clients this way in its Help Center: "Partner categories are a way to identify and reach the right people with the right message on Facebook, based on their activity off of Facebook. For example, you can use these targeting options to show your ads to people who are heavy buyers of health and wellness products, or who have taken actions that indicate they may be shopping for a new car.[9] Also in the Help Center it goes on to say "you can use partner categories with other Facebook targeting options" as well as, "We've built partner categories with our partners using their U.S. records."[10]

**Leveraging Offsite and Facebook User Information for Persistent Identification and Failure to Provide Effective Tools to Address User Privacy**

Facebook's "Bring Your Own Data" concept is central to the tying of covered information to vast amounts of data off of Facebook, allowing its advertisers and data partners to leverage as much private information as possible on individual users. Users do not have access to the information about what's collected and how it really works on the Exchange, despite Facebook's claims to the contrary. For example, a review on the partner websites reveals that "[w]ith FBX, Facebook has enabled marketers to import their own customer & intent data … . Facebook allows each marketer to 'Bring Your Own Data.' If a shopper has shown strong interest in a particular pair of Jimmy Choos on Nordstrom, we can show precisely that user exactly that pair of shoes. Both ad creative and bid pricing decisions are made at the level of the individual user, in real time."[11]

A Facebook user would have to review closely what Facebook says about each of its providers (i.e., click on "view profile" in their listing), and also analyze what the partner

---

[8] https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature

[9] https://www.facebook.com/help/459892990722543/; https://www.facebook.com/help/353223368111533

[10] https://www.facebook.com/help/459892990722543; https://www.facebook.com/help/357737337665825

[11] http://tellapart.com/early-results-from-facebook-exchange-show-strong-roi; http://tellaparteng.tumblr.com/post/49819416852/early-results-facebook-exchange

company says on its own site in order to have even a limited understanding of how the two companies work together to track that user.[12] Looking only at Facebook's descriptions misleads a reasonable reader. Facebook's site for Turn, for example, tells users that "Turn delivers real-time insights that transform the way leading advertising agencies and marketers make decisions."[13] It also cryptically identifies that Turn is involved in "financial services" marketing.[14] But when one goes to Turn's Facebook-related marketing page, the picture it portrays about how it uses user data is much different: "Turn Campaign Suite now enables you to perform custom audience targeting on Facebook, where consumers spend more time than anywhere else on the web. … [T]o run your Facebook Exchange advertising, you can use the same data sources and sophisticated audience designs for behavioral targeting, demographic targeting, and remarketing as you do for video, mobile, and other display inventory."[15] Essentially, Turn enables companies with existing data on users to target them *individually* on the Facebook platform. The FTC needs to examine, in terms of privacy, what user-related information Turn receives from Facebook and what is also shared with its clients and partners.[16]

Facebook is working with financial advertisers that have privacy and consumer protection consequences for users. As one report concerning a recent presentation to the ABA by Facebook's head of global marketing for financial services, Neil Hintz, explained, "You don't have to tell Facebook what financial products this pool of people has or doesn't have—they don't care. All Facebook needs to know is that you've identified a type of consumer you'd like to focus on. Facebook uses your list to find users in its system attached to the email addresses and phone numbers you've supplied. Facebook can then build a profile of other users who match the "digital accountholder" segment you've defined. And Hiltz says you can do this with astonishing precision. "Facebook ads are 90% accurate with our native targeting products — using geo, demo, interest, smartphone, etc., as variables. We can layer this targeting with the bank's data to gain even more efficiency," Hiltz explains. "The 'match rates' between the bank data tables and Facebook audience tables are contingent upon the quality of the bank's dataset,"

---

[12] See http://www.facebook-pmdcenter.com/fbx

[13] http://www.facebook-pmdcenter.com/profiles/view/11093

[14] http://www.facebook-pmdcenter.com/profiles/view/11093

[15] http://www.turn.com/solutions/advertising/facebook-advertising; http://www.turn.com/casestudies/turn-campaign-suite-delivers-strong-roi-financial-services-advertiser; For an overview of the data tools Facebook makes available to advertisers and marketers, see its "Power Editor" feature for developers: https://www.facebook.com/help/194355723944655/. It is important for the commission to address that many of Facebook's exchange data partners are engaged in financial marketing. Through links at Power Editor one accesses developer and advertiser data sheets on Facebook products, such as "Custom Audiences: Creation & Management," "Sponsored Results."

[16] The commission should also investigate how Facebook's data partners gather other data. For example, Turn has far-reaching relationships with numerous data providers that use offline and online data. They include many companies involved in financial services marketing, including Acxiom, Alliant, Epsilon, and MasterCard. http://www.turn.com/en-gb/data-partners

Hiltz continues. "We can also work with trusted third-party data providers. We have existing relationships with Acxiom, Epsilon, and DataLogix, and are signing up even more data providers going … ."[17]

Adroll's work also illustrates how Facebook's claims that users' identity isn't shared with advertisers are imprecise—if not disingenuous. The goal of Facebook retargeting (to "serve ads to potential customers who've previously visited their website as they browse the web and Facebook," according to AdRoll) is to bring them back to the marketer's site—a tactic designed to collect further data from a user.[18] When Facebook facilitates retargeting it is implicitly misleading users whom it has told it would not share their information with advertisers.[19] Facebook also doesn't explain to users the impact on their financial privacy of data partner AdRoll's focus on "financial services."[20] Facebook is also working with online lead generation companies—which collect information on users without meaningful disclosure and sell it to loan and other financial companies that often prey on consumers—to help them target its users. As one lead generator using Facebook explained they "can take offline data, such as email addresses or phone numbers, from an advertiser's CRM or other sources, and find those users on Facebook. … [W]ith custom audiences we're able to expand our online targeting to users we historically were unable to identify online … . For a company like DoublePositive, who works with millions of email addresses and phone numbers, this one is huge."[21]

One would not learn much of anything about one's data privacy from Facebook's description of data partner Appnexus.[22] If a Facebook user concerned about privacy went to the Appnexus site, he or she might discover that Appnexus uses a broad range of data gleaned from many other companies for its targeting, which can be brought into the Facebook Exchange system by the company.[23] For example, it has relationships with Bluekai, eXelate, Liveramp, Lotame, Neustar, Proximic, and many more.[24] Similarly, a Facebook user eventually finding Criteo on Facebook's site would learn that it is "user centric and relies on product level recommendation algorithms able to select the right banner at the right time."[25] Should an abnormally diligent Facebook user read Criteo's

---

[17] http://thefinancialbrand.com/33967/facebook-advertising-in-banking/

[18] http://www.scribd.com/doc/151089776/FBX-by-the-Numbers-June-2013; http://pages.adroll.com/fbx_news_feed_report.html; http://www.scribd.com/doc/151089776/FBX-by-the-Numbers-June-2013

[19] http://blog.adroll.com/reengage-customers-facebookexchange

[20] http://www.facebook-pmdcenter.com/profiles/view/11098

[21] http://doublepositiveblogs.com/blog/page/3/

[22] http://www.facebook-pmdcenter.com/profiles/view/11087. The only seemingly descriptive words in the profile are "offers user targeting."

[23] http://www.appnexus.com

[24] http://appnexus.com/appnexus-apps; Compare this with Facebook's approved description of Appnexus: http://www.facebook-pmdcenter.com/profiles/view/11087

[25] http://www.facebook-pmdcenter.com/profiles/view/11099

recent IPO filing with the SEC, he or she would discover that the company "typically [has] real-time access to the products or services a customer has viewed, researched or bought from them and we continuously receive updated information on approximately 700 million individual products or services, including pricing, images and descriptions."[26] Knowing this, it is apparent that Facebook's description of this company as "user centric" leaves much to be desired.

The story is the same with other partners as well. One would have to review X+1 documentation to see that it incorporates a wide range of "audience data" for Facebook and related targeting.[27]

**Sharing Covered Information through Cookie-connected Data**

In addition to being largely opaque to the average user, these partnerships connect covered information with users' input into search engines all over the Internet. Facebook has added a user's search history into its Exchange through its relationship with Chango, which "maintains user profiles linked to search activity on approximately 300 million people in North America" and brings "search intent" data to Facebook from Google and Bing, among others.[28] In another example of Facebook's failure to explain how user data are used for tracking and targeting, one would have to review Facebook Exchange materials on Chango's website to learn what privacy users lose in this deal. Cookie-connected data are "collected about each individual prior to their arrival on Facebook … ," and then used to link advertisers and their targets.[29] Facebook Exchange enables a cookie-end user to be targeted on its platform and also pursued via retargeting. (Although Chango, like others, claims the user cookie data are "anonymous," the Commission increasingly recognizes that such software identifies an individual user).[30] Facebook partner Chango describes for clients—not Facebook users—how Programmatic Site Retargeting (PSR) strategies involving Facebook Exchange works: "PSR incorporates visitor behavior from a wide range of sources, including customer profiles, shipping addresses, items in cart. … [A] cloud-based user profile [is assigned] to each visitor. These profiles allow marketers to gather data on an anonymous user in real time. … [W]e make this data actionable by giving a 'visitor score' to each of the cloud-based profiles … ." [31] It is questionable what "anonymous" could mean in a situation where the

---

[26] http://www.sec.gov/Archives/edgar/data/1576427/000119312513369592/d541385df1.htm

[27] http://www.xplusone.net/products/origin-data-management-platform

[28] http://www.adexchanger.com/social-media/facebook-exchange-adds-search-intent-data-as-chango-joins-partner-list/

[29] http://resources.chango.com/rs/changoinc/images/Chango_FBX_Whitepaper.pdf

[30] http://www.ftc.gov/opa/2013/07/coppa.shtm; http://www.ftc.gov/os/caselist/1023185/index.shtm

[31] "The Facebook Exchange Handbook." Available via: http://www.facebook-pmdcenter.com/profiles/view/11127; http://www.adexchanger.com/social-media/facebook-exchange-adds-search-intent-data-as-chango-joins-partner-list; http://www.facebook-pmdcenter.com/profiles/view/11127; Facebook also enables "realtime dynamic ad creative" changes that takes advantage of the data to further influence users. Given that "Upon receiving a

company claims to have that much information on a user as it follows that user through Facebook. Even if the company acts as if this user's profile is their proprietary data and doesn't regularly share it, the provision of covered information to advertisers is what Facebook said it would not allow, and yet it seems to be Chango's business model.

**Sharing User Information through Email Address Matching**

Facebook's proposed Data Use policy is designed to enable its recent expanded use of email addresses for targeting users. Facebook relies on email addresses as a key part of its data retargeting in its Facebook Exchange and Partner Categories products.[32] Facebook claims that it has an anonymous method of "hashing" email addresses and only giving advertisers a user's information for linking if that anonymous system produces a match. However, Facebook matches users to a much broader data set in many instances, as Facebook notes to developers: "Custom audiences allow advertisers to target their Sponsored Story or ad to *a specific set of users* with whom they have already established a relationship on/off Facebook. Audiences can be defined by either user email address, Facebook UIDs, user phone numbers, app user IDs, or Apple's IDFA."[33] There is nothing anonymous about this method of identifying Facebook users, and linking covered information to these outside data sets makes Facebook liable for all of this information sharing, as the definition of "covered information" includes "any information combined with" any covered information in a user profile.

Facebook explains to marketers this more candid view of Custom Audiences than it does to users:

> Custom audiences let marketers find their offline audiences among Facebook users. Using email addresses, phone numbers, Facebook user IDs or app user ID's to make the match, you can now find the exact people you want to talk to, in custom audiences that are defined by what you already know.
>
> This means that in addition to targeting the types of people you want to reach among the Facebook population, you can now also reach segments of specific people based on information you have about your own, offline audiences.

---

bid request, the advertiser must reply within 120 ms," the speed of the process and its implications for Facebook user privacy should be addressed in its Data policy. https://developers.facebook.com/docs/reference/ads-api/rtb/#cookie_matching; https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125; https://www.facebook.com/about/privacy/other

[32] https://developers.facebook.com/docs/reference/ads-api/rtb/; http://techcrunch.com/2012/06/13/facebook-exchange/; https://developers.facebook.com/docs/reference/ads-api/partnercategories/

[33] https://developers.facebook.com/docs/reference/ads-api/custom-audience-targeting

> You can create a custom audience representing any group of customers or prospect list that you'd like to reach with targeted Facebook Ads. For example, you could run a campaign to get more likes for your Page, targeted at your current customers who have not yet liked your Page.[34]

Facebook also explains how marketers can use Custom Audiences to find users:

> First, identify the groups of customers you'd like to talk to within your contact management system. This might be subsets of current customers, prospects, loyalty club members, current or lapsed users—anyone you want to reach with highly targeted messages.
>
> Then use power editor to find these people on Facebook. Input an email or phone list representing your segments into the power editor. The list will be hashed before being sent to Facebook. The system will match the encrypted data against Facebook's active users, and build a custom audience in your account with everyone that matches your list.[35]

Facebook claims it doesn't share user data with third parties, but it invites those third parties to provide it with a great amount of user data, so Facebook can target specific users; it also sets the stage for the third party to likely learn that person's identity via retargeting.

**Sharing User information through App User IDs**

Facebook also fails to explain to users how its new mobile device-targeting service for Custom Audiences works. In May 2013, Facebook

> released a new custom audience solution designed specifically for mobile app developers: app user IDs … . App user IDs extend the benefits of custom audience targeting to mobile in order to solve some of the unique challenges marketers face when remarketing and reengaging their app user bases … . Adding app user IDs as an additional targeting field for custom audiences solves this challenge, allowing developers to request an encrypted ID from Facebook when someone uses their app.
>
> App developers can now reach and reengage their current user base even if they have not registered with the mobile app upon installing it. For example, a retailer can reach and reengage a person on Facebook who installed their mobile app and browsed particular products, but who may not have necessarily registered their email address or phone number with the retailer … .

[34] https://www.facebook.com/help/341425252616329

[35] https://www.facebook.com/help/491619737533280

> Not only can companies with mobile apps now remarket to their user bases with a laser focus with app user IDs, they can do so across devices … . Thanks to custom audience targeting with app user IDs, marketers can now effectively connect their remarketing and reengagement efforts on mobile to desktop.[36]

Facebook explains this process in the following manner: "When someone uses your app, you can make a request to Facebook's servers to request an ID be generated … . Facebook will return an encrypted ID for that person. (It can also return nothing depending on a person's choice … .). … You then send that ID to your server in order to use it later for custom targeting … . Each call to Facebook's server to generate an app user ID will *generate a different ID*. Although multiple calls will end up targeting the same person."[37] Once again, Facebook hides behind misleading rhetoric that "no personal customer information (such as demographic, Facebook ID, etc.) is shared with you or advertisers … ."[38] The reality is that the advertiser/developer has shared user information with Facebook, may be able to then use the process to gather PII or related data, and that the social network has gathered additional information about its users. Facebook's claim that it doesn't share user information with third parties is both technically incorrect and perverse.

The social network has created a system where it is given abundant personal and data-related information on individual users, is freely able to merge it with its own data, and then has a more robust—and likely ongoing—ability to track and further gather and use their information. Facebook also supplies third parties with user information that they can use to identify specific Facebook users and their activities across devices and platforms. All of this is done without the meaningful ability of a user either to understand or to control how the system operates.

**Facebook and App Data**

In its proposed Data Use Policy, Facebook adds the phrases "use or are running" and "or about" Facebook, additions that reflect its recent mobile application ("app") data practice changes, which are now Facebook's focus in future app development.[39] This Last Fall Facebook opened up its "mobile app install ads" to all developers, which are targeted ads designed to trigger users to download apps from developers.[40] Facebook urged developers to "hyper-target" the app-install ads, which can use email, phone number, and

---

[36] http://www.nanigans.com/2013/05/21/mobile-ad-targeting-facebook-custom-audiences-app-user-ids/

[37] https://developers.facebook.com/docs/ads-for-apps/custom-audiences-for-mobile-apps/

[38] https://developers.facebook.com/docs/ads-for-apps/custom-audiences-for-mobile-apps/

[39] https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851585_445264755581605_1677569786_n.pdf

[40] https://developers.facebook.com/blog/post/2012/10/17/drive-installs-and-discovery-with-mobile-app-install-ads/

Facebook User ID's as well.[41] Hence developers are using covered information expressly for advertisement targeting, contrary to any statements that such information remains hidden from advertisers.

Facebook has expanded the tracking of users through more than a dozen "mobile measurement" data partners.[42] For example, its users are unaware what partner Kontagent does and what the partnership between these companies may mean for user privacy and consumer protection. In announcing the relationship, Kontagent explained that "customers who purchase the new mobile app install ad unit on Facebook will, through our Mobile Marketing Analytics, be able to gain deeper insights into levels of user, including engagement, retention, and monetization … . Kontagent *k*Suite DataMine™ users will be able to analyze the behavior of customers from this new channel down to the most granular level possible."[43] The "data insights" Kontagent provides are for companies specializing in, among other things, financial services.[44] The FTC will have to look at this "most granular" service that tracks individuals' behavior, and see to what extent Facebook users are being made identifiable by these partnerships. The privacy implications of such close tracking must be explored. The Commission should also note reports that "Facebook's mobile app install ad unit is performing well for Financial Services."[45]

Facebook mobile measurement partner Kochava uses device fingerprinting to help "track even the untrackable," something also not told to Facebook users at any point.[46] It explains that "[b]y using a variety of algorithms which incorporate geo-location, carrier information as well as device information, we can match clicks to installs with an ~85% accuracy rate." The company uses a broad range of identifiers to help it track users across platforms and services.[47] The use of such techniques that enable the identification of users regardless of where they are online, including mobile phones or PCs, and their connection to Facebook mobile and geo-locational practices raise questions about the efficacy of the consent degree to address contemporary practices. Thus the Commission must review the data collection practices of the mobile measurement partners in light of

---

[41] http://www.ampush.com/the-facebook-mobile-app-install-ad-checklist/; https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851563_128604107334977_1765173912_n.pdf

[42] https://developers.facebook.com/preferredmarketingdevelopers/mobile/measurement/

[43] http://www.kontagent.com/kaleidoscope/2012/11/14/kontagent-facebook-enable-mobile-marketers-to-run-more-effective-campaigns/

[44] https://developers.facebook.com/preferredmarketingdevelopers/mobile/measurement/#kontagent

[45] http://www.facebook-download.com/uk/2013/03/mobile-success/

[46] https://developers.facebook.com/preferredmarketingdevelopers/mobile/measurement/#kochava; https://kochava.com. See also, e.g., https://www.facebook.com/help/www/248716141830800?rdrhc; https://www.facebook.com/help/218345114850283.

[47] http://support.kochava.com/customer/portal/articles/960425-server-to-server-integration; http://www.mobyaffiliates.com/mobile-app-marketing/kochava/

what Facebook's consent decree commitment, including its privacy-related controls for mobile apps.

In another mobile-related privacy development, Facebook announced to developers on 18 September 2013 that "[i]n addition to using, in a privacy safe way, current customers' emails, phone numbers, and Facebook UIDs, you can also upload and target specific types of IDs generated from your mobile app to reach relevant people on Facebook."[48] It explained that "you can also reach your mobile customers by leveraging Apple's standard advertising identifier, iOS IDFAs. For example, you can upload a list of your existing customers' iOS IDFAs into Power Editor, and reach them with relevant information about your app such as an important update. The ability to upload Mobile Advertiser IDs (iOS IDFAs or App User IDs) is available in Power Editor or via our APIs. Go to our tutorial to learn about all of your options for how you may reach your mobile app users through our custom audiences."[49] Considering Facebook's aforementioned departures from truthful descriptions, it is incumbent upon the FTC to review the use of these identifiers rather than taking the company at its word (i.e., "in a privacy safe way," which is too vague to provide assurances in any case).

**Sharing User Information by Creating New Personally Identifiable IDs**

As already described, much of Facebook's matching practices result in sharing covered information, already existing personally identifiable information, or creating new personally identifiable IDs for unique users. To users, such services as Facebook Exchange are described as totally benign. Facebook, in a September 2012 post about "protect[ing] your privacy," says that it gives its third-party data providers an "ID number (separate from your Facebook ID) for each visitor's browser. If someone then visits Facebook and his or her browser has that ID, we notify the service provider, who tells us when a marketer wants to show a particular ad."[50] Facebook claims to its users that this system "allows marketers to show you ads relevant to your existing relationship with them—and without them needing to send us any personal information about you."[51] Facebook's post provides a link regarding its third-party data providers, but it doesn't identify them.

In the same post Facebook describes its method of matching email addresses so users can be targeted via its "Custom Audiences" ad product.[52] It explains that "[t]hese hashes [of

---

[48] http://developers.facebook.com/blog/post/2013/09/18/platform-updates--facebook-ios-sdk-3-8--larger-images-for-link-page-posts--and-custom-audiences-upda/

[49] https://developers.facebook.com/blog/post/2013/09/18/platform-updates--facebook-ios-sdk-3-8--larger-images-for-link-page-posts--and-custom-audiences-upda/

[50] https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125

[51] https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125

[52] https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125

email addresses] are bits of text that uniquely identify a piece of data (such as an email address) but are designed to protect against reverse engineering which would reveal that data. Since Facebook and [a representative online] store use the same method to create each hash, we can compare the store's hashes to hashes of addresses in our records and show the ad to any group of users that match."[53] But Facebook tells its Facebook Exchange clients another story—that they can "use online, cookie based user intent data to deliver ads [and] leverage your own consumer intent data."[54] Facebook urges marketers to use "their own consumer intent data from across the web."[55] Illustrating how Facebook utilizes a range of digital data-related marketing practices that impact a user's privacy without meaningful disclosure, it urges data-focused clients to implement on its Exchange "multi-touch attribution, view-through conversions, global frequency capping, day-parting, … creative optimization [and] retargeting."[56] The use of such digital marketing practices involves a range of data collection practices, and reflects the capabilities of Facebook and its third parties to gather more data and non-transparently influence a user's privacy decision-making.[57]

For Ad Exchange clients, Facebook explains its cookie matching process in the following manner: "FBX partners will HTTP 302 redirect from their pixel on an advertiser's site to Facebook's cookie-matching endpoint … . FBX Partners should specify two redirect endpoints if they wish to receive matched/unmatched responses. The Facebook cookie sync endpoint will redirect to one of the two endpoints based on the result of the match … ."[58] The use of "IP address as string with last byte masked" of users needs to be evaluated to determine whether, in combination with other data, user information is being shared without meaningful consent.[59] CDD believes that this process may convey or facilitate contact information with the user, and needs to be evaluated—at both the technical and contractual levels—for meaningful anonymity. Facebook also permits

---

[53] https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125

[54] https://www.facebook-studio.com/fbassets/resource/66/FacebookExchange20120913

[55] https://www.facebook-studio.com/fbassets/resource/66/FacebookExchange20120913

[56] http://marketingland.com/facebook-ad-exchange-fbx-opens-for-business-with-16-partners-21490

[57] See for example, http://www.facebook-download.com/uk/2013/04/attribution-qubit/; http://www.kenshoo.com/quantifying-multi-touch-attribution/; http://www.nanigans.com/2013/08/28/facebook-exchange-10-steps-to-boost-conversions/. The Commission should also assess the data collection being processed on the Facebook platform by attribution companies such as Visual IQ, which explains that it has been "tracking advertising activity on Facebook in any and every way it can be tracked since the social network first offered advertising. Our unique, proprietary, pixel-less tracking system pulls in data from all of our clients' digital marketing tools and all of their data sources—including Facebook." http://www.visualiq.com/content/visual-iq-perspective-four-crucial-takeaways-attribution-facebook-roi; http://www.visualiq.com/content/viq-video-page

[58] https://developers.facebook.com/docs/reference/ads-api/rtb/

[59] https://developers.facebook.com/docs/reference/ads-api/rtb/

outside marketers to use view through pixels "to facilitate tracking on third-party analytics systems (and associated features like multi-touch attribution, global frequency capping, etc.) FBX allows partners to render view tags alongside a FBX impression."[60] CDD also believes that the use of Facebook and industry-wide tracking analytics may enable user identification and contact.

**No Meaningful Opt-Out**

One has to be knowledgeable about Facebook's exchange system, and the role of third-party data companies in particular, in order to address its privacy implications. Users are presented with information that makes it appear simple and transparent. For example, Facebook claims in its 30 September 2012 post that "[w]hen we show an FBX ad on Facebook, it includes an 'X' link that lets you provide feedback about ads. We also provide a link that lets you learn more about and choose to opt out of future ads from the service provider responsible for that ad."[61] But rather than giving meaningful information, this process merely directs users to the companies' boilerplate statements about opting out and general information-use practices.

When one clicks on the X, as we did for a United Airlines ad that was placed by a company named TURN, one goes to an "opt-Out of Turn Ad Targeting" page that doesn't provide a Facebook user any relevant information on what's collected or how. The Facebook-linked opt-out does not inform the user of the data sources, targeting categories (such as finance), subsequent data profile sharing, etc. It is, in essence, a blank screen that fails to provide essential information for the expression of meaningful choice.

Similarly, another Facebook ad connects one to a section on Rocket Fuel's privacy page, which leads to an opt-out statement and links: "Opting Out: It's a virtuous cycle we're happy to be part of, and we hope you're equally happy with your role in this endeavor. But if you're not, please click here to opt out of personalized ads based on the Rocket Fuel cookie, or here to opt out of other personalized advertising via the Network Advertising Initiative's opt-out page. If you opt out, you'll still see ads from us online, and we'll still do our best to serve the most relevant ads we can. We just won't know it's you, so we won't be able to apply any of your ad preferences."[62] These pages are not meant to inform users, but to convince them that opting out is either futile or unimportant. This does not give users information they can assess and weigh in order to make informed decisions about their online privacy

**Can You Protect Your Privacy?**

Facebook affirmatively states that users can understand and protect their privacy in this new environment: "As part of working with Facebook, we've set up these partnerships in a way that people who use Facebook can understand how this advertising works and have

---

[60] https://developers.facebook.com/docs/reference/ads-api/rtb/

[61] https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125

[62] http://rocketfuel.com/privacy-policy

the ability to control it."[63] Facebook describes the various "comprehensive" controls that are available, such as "inline transparency," "enhanced disclosures, and "data access tools."[64] Facebook's definition of these terms, and what they really mean, need to be questioned by the FTC. Facebook and its partners fail to provide the promised transparency, "enhanced disclosures" and controls. For example, the Facebook help center page for users listing its third-party partners also claims that users can "[l]earn more about these providers and the choices they offer."[65] But as with the Sponsored Stories disclosure in the Statement of Rights and Responsibilities (discussed in the accompanying analysis memorandum), users are given a very limited and largely meaningless view of what is collected and how it may be used.

For example, the link for Turn takes one to an opt-out page, which doesn't disclose anything about its data-use practices; in other words, there are no "enhanced disclosures."[66] On Turn's page opt-outs are offered for the Digital Advertising Alliance and NAI self-regulatory systems and two undefined links related to Turn ("Opt out of Turn, Opt out of TURN Corporate Marketing").[67] A user would not be able to make informed privacy choices in this situation because there is no meaningful explanation of what these different links will do, nor of what information Turn might already have. Nowhere listed on Facebook's Third Party Service Providers page or the link to Turn's opt out is how Turn's major data trading desk partners are working with Facebook. According to AdExchanger.com, these include "Omnicom's Accuen, Aegis's Amnet and IPG's Mediabrands Audience Platform."[68] As the Commission knows, these are user-data "trading desks" from some of the largest advertising firms in the world. Similarly, Facebook's link to data partner Xaxis (WPP) takes one to a privacy policy that says it does not collect PII.[69] For those knowledgeable about the data business, Xaxis is known as the "World's Largest Pool of Audience Data," offering "More Consumer Touchpoints than Any Other in the Industry."[70] Xaxis's use of data enables it to target users "with an unprecedented level of precision across multiple digital platforms."[71] The disconnect

---

[63] https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729

[64] https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729

[65] https://fb-lt.facebook.com/help/www/133547810119620

[66] http://www.turn.com/privacy/optout

[67] http://www.turn.com/privacy/optout

[68] http://www.adexchanger.com/ad-exchange-news/fbx-ftw-partners-share-results-as-facebook-exchange-exits-beta/

[69] https://fb-lt.facebook.com/help/www/133547810119620

[70] http://www.xaxis.com/page/privacy-policy

[71] http://www.xaxis.com/news/view/groupm-launches-xaxis-ad-industrys-most-comprehensive-audience-buying-. In this month's *MIT Technology Review*, both Xaxis and Turn executives are quoted about how they operate with data. http://www.technologyreview.com/view/518556/a-clearer-picture-companies-define-how-they-add-value-to-the-ad-tech-space/

between this business model and the idea that the company avoids identifying individuals is something the FTC should examine to understand how Facebook is allowing tracking by Xaxis. [72]

Facebook data partner DataXu's link also takes users to a privacy opt-out page, which first says it is a site approved by TRUSTe, encouraging individuals to trust this showing of self-regulation.[73] Opt-out information is far below on the page and does not offer enhanced disclosures or other controls that Facebook said would be present.[74] Despite Facebook's stated commitment to transparency and control, its users concerned about their privacy would have to be experts in digital marketing to know that DataXu tells clients they can "Deploy data on Facebook to deliver highly relevant messages to target audiences."[75] Nor are everyday Facebook users told, despite Facebook's promise to the FTC to provide genuine privacy settings, that data collected from them by DataXu involve the use of "direct A/B tests to compare our results on DataXu for Facebook Exchange to the results we garner from native Facebook targeting as well."[76] (Such testing impacts users' privacy choices). Nor are Facebook users informed by the DataXu privacy link that the company's data partners include MasterCard, Bluekai, eXelate, Transunion, Lotame, and others about the privacy implications.[77] The FTC should look at these revelations in light of the Order to discover if omissions of this information amounts to misleading users about how data are used.

One Facebook partner withholds information from users that it had to give to Members of Congress who were investigating data brokers; this reluctance to provide the same quality of information is significant. Epsilon's link from Facebook goes to a complex and obtuse "Marketing and Consumer Choice" page ("Epsilon provides companies the tools to bring relevant and targeted marketing offers to consumers") that provides insufficient disclosure of its practices and is misleading for being overly vague.[78] Epsilon doesn't tell Facebook users the categories of data it uses, information that was explained in its letter to Rep. Joe Barton and then-Rep. Ed Markey.[79] In a 14 August 2012 letter responding to an inquiry related to databroker information collection, Epsilon listed some of the "public

---

[72] http://www.businesswire.com/news/home/20110627005401/en/GroupM-Launches-Xaxis-—-Ad-Industry's-Comprehensive

[73] https://fb-lt.facebook.com/help/www/133547810119620; http://www.dataxu.com/about-us/privacy/data-collection-platform/

[74] http://www.dataxu.com/about-us/privacy/data-collection-platform

[75] http://www.dataxu.com/facebook-preferred-marketing-developer-dataxu-announces-support-facebook-exchange-campaigns/

[76] http://www.dataxu.com/facebook-preferred-marketing-developer-dataxu-announces-support-facebook-exchange-campaigns/

[77] http://www.dataxu.com/partners/partner

[78] http://www.epsilon.com/consumer-preference-center

[79] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

and private sources and uses" for its data—something Facebook users aren't informed.[80] These sources include data from "federal and state governmental agencies, catalog and retail companies, charities, magazines, retailers, utility companies, marketers, and other information brokers."[81] It also includes "public property records, telephone directories and certain public information posted to social media sites."[82] From this limited disclosure, it can be seen that there is nothing anonymous about the information this company is collecting: these are records tied to names, addresses, and other personal information about people.[83] Epsilon also gathers and uses geographic, demographic, financial and interest data, and household purchase information—just a few of the 22 primary categories.[84] Epsilon admits that it "utilize[s] third parties on behalf of its clients" to collect social media data, including "tweets, posts, comments, likes, shares and recommendations."[85] These can include "user IDs, names, ages, genders, hometown location, languages and numbers of social connections."[86] Nevertheless, Facebook's link to Epsilon's privacy page does not convey the range of data that can be used to target and track users on Facebook and off the site.[87] For example, Facebook users concerned about their finances would surely want to be informed of, and given appropriate comprehensive controls over, Epsilon's use of financial data. This is especially a concern in light of the linkage of financial data and Facebook: "Facebook advertisers can target people who currently have an auto loan."[88]

Finally, Acxiom's link from Facebook goes to a page without clear description of data use or any other company practices, although it does off an opt-out.[89] Users see this phrase at the top of the page, designed to encourage them to allow continued collection:

> Opting out, or choosing to have data about you removed from Acxiom's marketing data products, will reduce the amount of unsolicited telemarketing, direct-mail and/or email offers you receive from companies with whom you have not done business. It may also reduce the relevance of offers you receive from companies with whom you have done business

---

[80] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf at

[81] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

[82] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

[83] Epsilon told the Congressmen that "due to the confidential nature and proprietary nature of our contracts with our sources, we are unable to provide the exact identities of these sources." http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

[84] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

[85] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

[86] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf

[87] See Epsilon link on https://fb-lt.facebook.com/help/www/133547810119620

[88] http://www.epsilon.com/pdf/Epsilon_Congressional_Response_8_14_2012.pdf; http://blog.adespresso.com/facebook-partner-categories-guide/

[89] https://isapps.acxiom.com/optout/optout.aspx

since our clients use these products to better understand what offers may be of interest to you.[90]

From that page, a Facebook user would not know how Axciom's data can be used to target them, let alone the privacy consequences of not opting out. One would have to be an industry insider to understand that "Acxiom data allows Facebook advertisers to target ads by:

- **Demographics:** If you choose to target by demographic data from Acxiom you will be able to reach people by "Home" which includes if the person is an owner, renter, their length of residents and so on. You can also target by household size (1 to 6 people).
- **Financials:** Targeting your Facebook Ads using Financial data from Acxiom allows you to reach bank card users, credit card users and investors. Within the credit card category you can segment your reach by gas/depertment store/retail store card, premium card, travel/entertainment card and upscale department store. You can also reach people based on their typical spending method (cash or credit).
- **Job Role:** Acxiom's categories allow you to target your Facebook ads by job role. There are a variety of different options you can choose from including: admin, white collar, blue collar, education, legal professional, financial professional, military, sales, student and more.This ability to target people based on their job may impact LinkedIn Ads, which have traditionally been where marketers go when they need to run a campaign towards specific job types.
- **Purchase History:** Using Acxiom's Purchasing category will allow marketers to target users based on what they are spending money on such as: gas, computer electronics, office supplies, travel services, vehicles and more.[91]

Acxiom's link from Facebook doesn't explain the data used or their privacy implications—which the company provided in a release for clients announcing the alliance earlier this year: "The Facebook-Acxiom partnership represents the combination of the social graph data Facebook advertisers can leverage plus, from Axciom, the interests and behaviors consumers have expressed and demonstrated outside Facebook."[92]

---

[90] https://isapps.acxiom.com/optout/optout.aspx

[91] http://blog.adespresso.com/facebook-partner-categories-guide/

[92] "Partner Categories Drive Better Results for Facebook Advertisers." Acxiom/Facebook 2013. Personal copy available upon request; see also: http://finance.yahoo.com/news/acxiom-facebook-improve-online-advertising-151000872.htm. Facebook also allows advertisers to use tags for Custom Audiences created by its newly acquired Atlas service, something not disclosed. See http://www.insidefacebook.com/2013/05/22/facebook-adds-atlas-view-tag-support-for-custom-audiences-and-partner-categories/. The use of Atlas enables advertisers to gather more data on users: "Universal Action Tags enable Atlas clients to add tracking pixels from ad networks, publishers, or other vendors to Atlas action tags that are already placed on advertiser websites." http://atlassolutions.com/universal-action-tag. Facebook COO Sheryl Sandberg explained, "We

This ability to "leverage" social information off of Facebook, which is covered information in the Order, is not disclosed in public documents that users can access. None of the three additional links on the Acxiom opt-out page that are said to provide additional information on its U.S. privacy policy and products work. See Acxiom's U.S. Products Privacy Policy; Acxiom's Marketing Products; What Consumers Should Know. Hence, the user is even deprived of boilerplate that the company once had linked to through its unhelpful opt-out page. This review of Acxiom's actual data practices against the information provided to users should spur FTC to hold Facebook accountable for giving companies like this access to covered information without clearly explaining this to users. The Commission needs to assess the Acxiom and Facebook data relationship, including recent developments in which the data company is helping expand user profiles beyond cookies to a much more robust data set.[93]

**Network Behavior**

Facebook says it now accesses users' network behavior information, but doesn't tell users what that means.[94] It has launched a "new tool designed to help telecommunications companies (carriers and operators) bridge the gap between sales, which occur primarily in stores, and ad impressions delivered on Facebook … . From this starting point, we can establish test and control groups to determine how and when an ad on Facebook correlates to certain actions, such as a group of people switching to new handsets, tablets or carriers."[95] In this program, Facebook "analyzes a users' [*sic*] mobile phones and wireless provider to see who switches handsets or carriers after looking at specific carrier-based and mobile handset-based ads."[96] This is again tracking users much more closely than the words in the official policy, "network behavior," might alert them to. The FTC should assess whether such close tracking and reporting back to telecom companies—who have plenty of PII on their users to begin with that could be combined with Facebook's reports through this tool—goes beyond what Facebook has admitted to in its official policies.

---

believe the Atlas platform will help us demonstrate even more clearly the connection between ad impressions and purchases." http://allfacebook.com/atlas-view-tags_b118182. The use of Atlas combined with Facebook enables much more granular tracking of users, through attribution methodologies. http://atlassolutions.com/community/blogpost/115191/atlas-blog/what-atlas-analytics-can-do-for-facebook-advertisers; http://allthingsd.com/20130219/the-reason-facebook-is-buying-atlas/. The FTC should also review the use of Facebook's "Viewtags" on privacy: https://developers.facebook.com/docs/reference/ads-api/adgroup/

[93] http://www.adexchanger.com/data-exchanges/wpp-plimsoll/#more-61289

[94] https://www.facebook.com/facebookforbusiness/news/outcome-measurement

[95] https://www.facebook.com/facebookforbusiness/news/outcome-measurement

[96] http://www.socialnewsdaily.com/16787/facebook-targets-mobile-service-providers/

**Exposing User Data by Connecting Data: Facebook's New "Entities Graph" is Significantly Changing Data Use**

Facebook is increasingly working to track people in everything they *do*, rather than simply advertising to them based on who they say they *are*. This graph analysis, which uses email addresses to help further verify a user's identity, is done without the conscious awareness or meaningful consent of users. Users may have some knowledge about how Facebook views what it calls the "social graph," but its Data Use policy doesn't make transparent what Facebook explains in a June 2013 engineering note that "one way we map them [users] is by traversing the graph of their friendships."[97] Facebook says its social graph now "comprises over 1 billion monthly active users, 600 million of who log in every day."[98] But these same people are likely unaware—and have not been meaningfully informed—about the ways Facebook uses related data to identify them through what it calls its "Entity Graph."[99] The system is a "gargantuan map of relationships," explained *Wired*.[100] "It provides a kind of digital signature for each Facebook user and the world he or she inhabits."[101] Facebook's data system learns about user behavior that is then made actionable, for advertisers and others.[102] As Facebook explained in its June 2013 post:

> People don't just have connections to other people—they may use Facebook to check in to restaurants and other points of interest, they might show their favorite books and movies on their timeline, and they may also list their high school, college and workplace. These 100+ billion connections form the *entity graph*.[103]

Users do not know that Facebook's data analytics machinery is continually using their information to construct algorithms designed to take advantage of this user-related information, and how they interact in the world (including actions involving the "like" button, check-ins, etc.).[104]

---

[97] https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920

[98] https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920

[99] *See* https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920

[100] http://www.wired.com/wiredenterprise/2013/07/entities-graph/

[101] http://www.wired.com/wiredenterprise/2013/07/entities-graph/

[102] http://www.socialnewsdaily.com/16787/facebook-targets-mobile-service-providers

[103] https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920

[104] https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920

Facebook engineers have "loaded millions of entries into the entity graph by simply watching what people do on Facebook. Entities such as colleges and employers are learned from data typed into profile pages; businesses, movies, fictional characters, and other concepts are learned from fan pages created by Facebook users … . Facebook is now littered with tiny nudges to encourage people to contribute more directly … ."[105] Facebook's new graph search product takes advantage of this graph-focused data analysis. Facebook's graph "includes the relationships between" users, the pages they view, and "other objects within the Facebook universe."[106] Each "entity, or node within the Facebook graph" is identified by "a unique number called a fbid (Facebook ID) [that] has a set of attributes, or metadata associated with it. The relationships between these nodes, called edges, contain their own metadata to describe the type of relationship between them."[107] Once everything has a tracking number, everyone can be tracked: "You can learn what entities are close to a certain location, liked by certain people, or otherwise tethered to a user through the social network's path of edges."[108] The FTC must look at this increased data availability and determine if it is going to get in the way of user privacy in ways that Facebook does not bring up.

**Other**

To understand better how Facebook works to advance the data-gathering activities of its major advertisers, the FTC should review The Facebook Studio Gallery, the actual operations of its preferred ad related developers, and other resources.[109]

---

[105] http://m.technologyreview.com/news/511591/facebook-nudges-users-to-catalog-the-real-world/

[106] http://arstechnica.com/information-technology/2013/03/knowing-the-score-how-facebooks-graph-search-knows-what-you-want/

[107] http://arstechnica.com/information-technology/2013/03/knowing-the-score-how-facebooks-graph-search-knows-what-you-want/

[108] http://arstechnica.com/information-technology/2013/03/knowing-the-score-how-facebooks-graph-search-knows-what-you-want/

[109] https://www.facebook-studio.com/gallery/; https://www.facebook-studio.com/directory; https://www.facebook-studio.com/education/index