Social Media Privacy, Security, and Tracking Evaluation and Analysis

Jason Brazeal, Adam Soto, Brayden Van Ackeren, and Kareem Williams

***Abstract*— In this paper we evaluate the security capabilities and mechanisms of leading social media companies and the potential impacts of data breaches. Facebook, Google+, Instagram, LinkedIn, and Twitter are all top 10 frequented social media sites, and all are exposed to constant attacks. Each company has dedicated data warehouses to the collection and storage of user information gained from these networks. We analyze the potential for a breach to occur, and outcomes of said breach based on previous system hacks.**

I. Introduction

The growth of technology has led to the rise of social media as the premier platform of entertainment. Some social media platforms see hundreds of millions of active users each month, each with information stored regarding their online activity. Information regarding users is held and stored by companies as one of their root sources of income. As companies store information the need for highly secure systems that minimize users risk for exposure to hackers and cybercriminals becomes a necessity for a company to stay relevant.

With increased data collection, users are placing more trust into, or have an increased ignorance toward, each individual company's protection of user activities. Most individuals see social media sites as platforms to access entertainment options, most without recognizing the true tracking nature of most of these free websites. As users become identifiable through data there is a call for higher protection standards from users. As companies develop and self-regulate data a questions come to mind regarding the safety of individual identity within these structures, particularly if there is a breach of the collected materials. The need for evaluation of the security capabilities and practices of multiple social media companies is necessary. Each company's security evaluation attempts to determine the potential privacy impact on users.

II. Methods of Evaluation

In order to properly analyze security and potential outcomes systems understanding and historical events must be considered. Cookies and privacy policies, web browser extensions, application programming interfaces, web traffic metrics and documented attacks will all be used to evaluate the security of Facebook, Google+, Instagram, LinkedIn, and Twitter. Companies are in a similar industry, so it is expected that there will be high levels of overlap across company methods, 3rd party contributors and implementation.

A. Cookie and Privacy Policy

Evaluation of the each company starts at the corresponding cookie and privacy policies. These policies give insight into user agreements, tracking of information, third party contributions, opt-out clauses, and recommendations users can follow to increase privacy.

B. Ghostery

Ghostery's web browser extension will be used to identify any well-known trackers placed on websites. Ghostery identifies source of tracker as well as the data the cookie is tracking. While this company has registered a large number of trackers, some smaller, nonregistered trackers may be missed because of the extension's reliance on users machines reporting and identifying browser cookies.

C. *Application Programming Interfaces (APIs).*

An Application Programming Interface (API) is a standard tool for social media websites to increase outside developer contributions. APIs can allow access to information, sometimes considered private, but generally with agreed terms of use. An evaluation of the APIs for each platform give insight into information third party developers' are able to access.

D. Web Traffic Metrics

SEMrush and Google Trends are primary tools for analysis of web traffic to the selected social media networks. Web traffic analysis will occur using metrics and graphics using SEMrush, an online search engine marketing resource that provides website traffic statistics and comparative analysis across multiple domains. Google Trends provides a timeline visualization of chosen news events.

E. Well Documented Attacks

After years of operation social media companies have developed large amounts of data regarding users that would prove valuable to unethical hackers. The trove of information has inspired constant attacks, some of which proved to be successful and became well documented. Analysis of highly reported attacks provides understanding of the implications of data breaches to user privacy.

III. Company Profiles

A. Facebook

Facebook is a social media company that has evolved for people to connect with one another. It was originally created for connecting college students, but has grown into the largest social media and one of the most frequented sites in the world. As a result, Facebook has now become a tech behemoth that has a variety of uses such as a communication platform for businesses, celebrities, customers, family, and friends. Essentially, Facebook at its core is a social network that links individuals and groups.

Facebook is also a leader in the use of analytics and data gathering for advertising and product/services improvement. In their private policy they describe the information that is collected on users. Essentially every piece of information is collected on every action committed by users such as device information per session, payment information, friends, and activities. Facebook primarily uses the information collected on users to continually improve Facebook products, personalize advertisements for users, and ensure safety and security.

Information is collected in a variety of ways, such as through cookies, which collect session and log information to third party analytics that track users' activities.

TABLE I
FACEBOOK TRACKING SOFTWARE AND DATA COLLECTORS

Tracking Software	Data Collected
Adobe Marketing Cloud Atlas Double Click by Google Neustar PlatformOne	Ad views, Analytics, Browser Information, Demographic Data, Hardware/Software Type, Interaction Data, Page Views, IP Address (EU PII), Search History,Clickstream Data, ClientBrowser Information, Cookie Data , Date/Time, Demographic Data, Hardware/Software Type, Interaction Data , Page Views, Serving Domains

This is a list of tracking software platforms and services (left) and data collected (right) that Facebook uses for third party analytics.

Facebook is also leader in security and has a variety of encryption practices in place to secure user information. Since 2011, Facebook has used HTTPS to ensure user information is secure. Additionally, Facebook utilizes TLS for email notifications with perfect forward secrecy and certificate validation. They also allow the use of OpenPGP for end-to-end encryption where users have the option for creating their own public keys and enabling OpenPGP for additional security. Facebook also uses social authentication instead a traditional captcha to verify user authenticity. As a result, users must verify a picture that contains a photo of a friend and name them. Users also have the ability to enable two-step authentication for logging into Facebook on an unknown device, where a security code is sent to the user's phone. Lastly, Facebook provides additional security by allowing access via Tor. Facebook offers an onion address where users can access the site through Tor and also delivers SSL on top to validate certificates exchanged between Facebook and the user.

B. Google+

Google users have access to a full suite of online applications with a single login, including Google+. Various posting channels are made available for subscribers and individual posts can be denoted as interesting to users who click a +1 icon. This icon reflects user interests and can be utilized to customize and present future content.

Although the parent domain is among the fastest websites to exceed one billion users, Google+ has tended to lag behind other social media outlets in terms of utility and usability for a broader audience. Their current user base sits near the 300 million mark. Although instant messaging and posting are made possible, this forum tends to be less naturally social.

Like other Google products, Google+ complies with Google privacy and security policies. Google began the process of doing away with SHA-1 in 2014 and announced that they would proactively support Microsoft's 2013 proposal to deprecate SHA-1. As of January 1, 2016, any code-signing interaction with Google requires SHA-256 as will all SSL certificates by January 1, 2017. In addition to single socket layer encryption and other transport layer security measures in place, Google has also implemented OAuth 2.0 tokenization and authorization measures. For all Google suite applications, Google adheres to RFC4880 and OpenPGP (pretty good privacy) standards.

These provide various security layers and methods of protection against multi-faceted potential exploits. However, as the Google family of products continually expands, they must devise end-to-end protections against savvy hackers looking for a back door to Google customer data and functionality.

Google's Privacy Policy emphasizes that they take user privacy protection very seriously and reinforce it throughout their organization's employee training and technology development.

The terms and conditions laid out on their privacy page also deal with information sharing, use of cookies, pattern recognition and other privacy concerns. Furthermore, Google allows for user configuration, deletion and takeout functions to customize information sharing and security. Although Google deploys cookies and other functions like image recognition to personalize the user experience, they support user preferences and follow applicable laws. They also aggregate information about transactions and analyze traffic to optimize site performance. Altogether, Google privacy is both configurable as well as standardized to provide enhanced supervision.

TABLE II
GOOGLE+ TRACKING SOFTWARE AND DATA COLLECTORS

Tracking Software	Data Collected
Double Click by Google	Ad Views, Analytics, Browser Information, Cookies Data, Date/Time, Demographic Data, Hadware/Software Type, Interaction Data, Page Views, Serving Domains, IP Address (EU PII), Search History, Location Based Data, Device ID (EU PII), PII(Phone Number)

This is a list of tracking software platforms and services (left) and data collected (right) that Google+ uses for third party analytics.

As with most online platforms, Google+ provides an application programming interface, or API, so that external apps can interact with the Google+ framework. This particular area is where OAUTH 2.0 tokens and SSL encryption are utilized to restrict authorized access. Regardless of access granted, password resets and payments are mostly off-limits, while granting fully trusted access to an app like Google Maps can allow for significant updates to Google+ user profile information.

Ultimately, Google+ security depends on existing systems and configured settings. In part, user security is a shared responsibility between the Google+ security measures and the information sharing settings set forth by the owner of each Google+ profile. Many aspects of a user's information known as resources can be accessed via the Google+ API. While this provides greater potential for helpful apps and integrated functionality, Google also maintains an overarching focus on end-to-end user security for all Google products.

C. *Instagram*

Instagram is a social media company that was created for people to share photos and videos with other users. Instagram was originally designed as a photography app that allowed people to share only photos and apply simple filters. Over the past few years Instagram has grown to become a mammoth social media company with over 300 million users that now serves as hub for social content.

As a subsidiary of Facebook, Instagram follows similar practices for tracking information and using analytics. Per their privacy policy, Instagram collects all information that is performed or created while using the product as well as device and session information. Through in-house analytics and third parties, information is used for improving their product, personalizing advertisements, and increasing their user-base.

Below is a table that describes the information that is collected as well as the third parties that help Instagram collect data:

TABLE III
INSTAGRAM TRACKING SOFTWARE AND DATA COLLECTORS

Tracking Software	Data Collected
Facebook Connect and Facebook Custom Audiences	Browser Information, Date/Time, Demographic Data,Hardware/Software Type, Internet Service Provider, Interaction Data, Page Views, IP Address (EU PII), Location Based Date)

This is a list of tracking software platforms and services (left) and data collected (right) that Instagram uses for third party analytics.

Over the past few years Instagram has made some strides in their security and encryption. Originally users were largely susceptible to attackers due to the use of HTTP. There has been an upgrade to HTTPS for mobile-web browsing, however aspects of the mobile app are still primarily HTTP. Currently direct messaging is the only fully encrypted portion of the mobile app. Two-factor authentication was implemented to battle against account hacks. Now users must provide an email and a phone number so that they can authenticate the account with a secret code sent to a mobile device and a message sent to email.

Instagram has come under fire for their general lack of security and has been primarily vulnerable to man in the middle attacks. Due to the use of HTTP, an attacker on an open Wi-Fi network is able to monitor a users session by viewing their traffic, the attacker is able to steal their session cookie and pose as the victim. This kind of attack is frequent and has been known to cause massive spam content, usually in the form of advertising for a particular product.

Instagram also received a tremendous amount of criticism due to a security flaw that allowed Wes Wineberg, an independent security researcher, to gain access to private Instagram data including: back-end source code, private user information, certificates, and more. Wineberg was able to find a backdoor into Instagram's Sensu-Admin Web application, from a Ruby flaw, that allowed him to accomplish remote code execution. From there, Wineberg was able to locate a configuration file that permitted access to their SQL database. He was easily able to break their bcrypt encryption and found that many employees utilized weak passwords such as "password" and "Instagram". Wineberg was then able to gain access to the company's AWS storage units where he then could maneuver through any user's account.

D. *LinkedIn*

LinkedIn is a social network for professionals and job seekers. The network has the intention of connecting similar individuals across the world for professional engagement. The basis for establishing a connection is rooted in commonality and therefore any requests ask for some linking trait that, often, can be validated.

LinkedIn's privacy policy introduces the information collected, whom collects data, information regarding personal details, and choices/obligations. The two main types of data collected by LinkedIn are profile data and marketing data. Profile data is any data that one inputs for their profile or places within the network, such as when LinkedIn asks for access to a person's contacts. Marketing data is what the company collects in order to create an optimized target marketing platform. Cookies, web beacons and other behind the scenes information collection methods are the main methods for accumulating this data. Third parties have their own privacy policy. This information is used solely for the purpose of providing one with an optimal profile in order to better connect with others on the network.

LinkedIn has had multiple highly publicized security vulnerabilities. In June 2012, there were over six million unsalted SHA-1 password hashes leaked. Immediate invalidation of millions of account passwords followed, with numerous sources hinting that the company planned a SHA-2 Hash upgrade. A 2014 free browser extension, SellHack, allowed users to identify LinkedIn users' emails accurately. The extension scanned profile information and ran valid web searches to identify connected emails without the authorized consent of the user attacked. LinkedIn attempted to shut down the extension, but all that was officially published was that the company condemned the add-on and asked that any data collected via SellHack be eliminated immediately. The most recent high profile attack was a Man in the Middle (MitM) breach that used SSL stripping to gain access to a profile once

on the same network as the attacker. LinkedIn never seemed to address the attack; some believe the company was already upgrading their standards to prevent such an attack. New Security procedures have been constantly questioned since the high profile incidents occurred 2014, and the company has revealed little information officially.

TABLE IV
LINKEDIN TRACKING SOFTWARE AND DATA COLLECTORS

Tracking Software	Data Collected
BlueKai by Oracle Double Click by Google Eloqua by Oracle Google Analytics Lotame QuantCast Full Circle Studies Cedexis AppNexus	Browser Information, Date/Time, Hardware/Software Type, Page Views , Serving Domains, Cookies Data, IP Address (EU PII), Clickstream Data,Demographic Data, Interaction Data, Location Based Data, Device ID (EU PII)) PII(Phone Number)

This is a list of tracking software platforms and services (left) and data collected (right) that LinkedIn uses for third party analytics

Data collection by LinkedIn is highly automated and used for the purpose of maximizing the profile experience, relevance and target advertising, none of the information is sold at any point.

E. Twitter

Twitter is a micro-blogging site that allows its users access to real-time information. From the latest weather updates to what your friend is eating for lunch, Twitter allows you to have this information instantly. Even though people of all ages can have a Twitter account, according to Investopedia, about 94 million of Twitter's 271 million users were between the ages of 18 and 29. With the number of users growing rapidly, Twitter found a way to monetize their micro-blogging site by advertising to their users. Companies and/or individuals can advertise on Twitter by 1) Promoting a Tweet, 2) Promoting an Account or 3) Promoting a Trend. Another revenue stream for Twitter is by selling access to its "Firehose". The Firehose is access to all of Twitter Public data, which typically increase by 500 million Tweets per day.

According to Twitter's privacy policy, the company receives user data through an assortment of avenues such as websites, SMS, email notifications, widgets, ads, etc. To help identify you as a Twitter user while you are searching the web, Twitter makes use of Cookies, Pixels and Local Storage technology. Cookies are used to learn how users are using Twitter services. Pixels are used to gauge what email or web content you have interacted with. Local storage is used to store information on your personal device to help distinguish each user experience based on previous interactions. By utilizing these technologies, Twitter is able to authenticate users, remember user preferences, perform analysis and research on its users, personalize the Twitter experience and help improve advertising. Twitter uses Cookies to store preferences such as preferred language and country of the user. Pixels are used to measure effectiveness of an add. Twitter uses local storage to track what parts of your timeline you have visited, so that it can present you with fresh recent content.

While we were not able to learn how Twitter stores the data it collects, we were able to get a peek inside using the Twitter API to see what data they do collect. The Twitter API gives us access to three Objects: Users, Tweets and Entities. The Users object contains mostly the information you give to Twitter when creating your account, as well as different boolean values used to control User Setting options. The Tweets object contains information about a specific tweet such the contributor, creation timestamp, location coordinates, favorites count, retweet count, ID and text. It also contains boolean values to track the interaction of users through Tweets like In reply to and quoted. The entities object stores metadata about the tweet such as users mentions, hashtags, URLs, and Images.

TABLE V
TWITTER TRACKING SOFTWARE AND DATA COLLECTORS

Tracking Software	Data Collected
Google Analytics Syndication Twitter Advertising	Ad Views, Analytics, Browser Information, Cookie Data , Date/Time, Demographic Data, Hardware/Software Type, Interaction Data , Page Views , Serving Domains, IP Address (EU PII), Search History, Location Based Data, Device ID (EU PII), PII (Phone Number)

This is a list of tracking software platforms and services (left) and data collected (right) that Twitter uses for third party analytics.

However, even though Twitter has a large amount of avenues to help tailor your Twitter experience, it respects the Do Not Track (DNT) flag that can be set in your browser. By selecting this option, you are opting out of participating in Twitter's tailored suggestions and ad experience. Although a user chooses to opt out pf the tailored Twitter experience, data will still be collected for analytic purposes such as counting how many users have seen a particular tweet.

Back in 2014, a XSS vulnerability was found in Twitter's desktop tool Tweetdeck. This specific vulnerability, found in certain versions, would execute JavaScript found in tweets. While this vulnerability was not maliciously exploited, it had the potential for Twitter Accounts to be hijacked. In 2013, Twitter was among other large American technology companies, that were victims of a data breach. This data breach exposed Usernames, Email Addresses, Session Tokens and Encrypted/Salted passwords of nearly 250,000 Twitter Accounts. To mitigate the effects of this breach, Twitter sent victims of this attack an email to reset their passwords, as well as revoked their current session tokens.

A potential attack that Twitter could face is due to the implementation of SHA-1 certificates. SHA-1 certificates have been deemed insecure by researchers and the security community.,An attack against SHA-1 has been created that only take 2^61 computations. With modern day computing, this attack would be possible below today's reasonable time standards. While Google has set an expiration date on these SHA-1 certificates of January 1, 2017, Twitter has not released a date for the completed conversion to SHA-256.

They are currently in the process of migrating to users to SHA-256 certificates as user certificates begin to expire.

TABLE VI
SUMMARY OF COMPANY PRACTICES

	Facebook	Google+	Instagram	LinkedIn	Twitter
Use Encryption:	HTTPS	SHA-256, SSL, OAuth2.0, OpenPGP	Primarily HTTP for Mobile, HTTPS for Web	Originally SHA-1 but transferring to SHA-256	HTTPS and SHA-1 but in process of upgrading to SHA-256
Major Attacks (Past 2 Years) :	Yes	No	Yes	Yes	Yes
Use Tracking Software	5	2	2	9	3
Share Data with 3rd Parties:	Advertising, selling user information (friends, age, relationship status etc)	Sells information such as Gmail content and search terms	Advertising	Targeted personalized advertisements	Sponsored and promoted tweets
Have Developer API:	Yes	Yes	Yes	Yes	Yes

A summary of practices of the five major social media companies.

IV. COMPANY SECURITY SUMMARY

Social media companies have been victims of different attacks over the past five years which have lead to major changes and upgrades across all platforms. Standard and implementation across these platforms differ as each companies prepares for varying types of attacks. Hashing login information with SHA-2 is becoming a prevelant practice as other methods are either being phase out or found to have insecurites. Communications are becoming more secure as companies update their platforms moving from HTTP to HTTPS. Each media source is putting privacy power into the hands of the user, with customizable viewship settings, user profile blocking abilities, and content sharing management. Each company has its own security development to best protect its products from attacks, but all companies have the same goal of preventing system breaches and data leaks. User security and privacy still rests some responsibility on the user themselves.

V. 3RD PARTY ANALYTICS AND TRACKING

Across the privacy policies and application programming interfaces of the social media sites studied, user tracking and data analytics are common themes. For various reasons, cookies and adware are installed on a social media user's computing device. Then, according to each platform's API and use terms, third party applications may obtain access to valuable consumer information that improves behavioral understanding and informs marketing efforts. Some tracking tools are focused on creating personalized offers for the host user based on traced preferences. Other mechanisms are focused on user actions and habits in order to predict their likelihood to purchase or engage certain pursuits. Depending on API permissions, app developers potentially have access to a user's profile data, location and IP address among other identifiers. Current privacy policies typically restrict externally sharing personally identifiable information; however, hackers continually seek to exploit any avenues to obtain the more sensitive information contained therein.

To this end, we examine the various tracking technologies used between these social media platforms in order to raise awareness of potentially accessible content.

TABLE VII
THIRD PARTY COOKIE TRACKERS

	Facebook	Google+	Instagram	LinkedIn	Twitter
Adobe Marketing					
Atlas					
BlueKai					
Comscore					
Double Click					
Eloqua					
Facebook Connect					
Facebook Custom Audiences					
Google AdWords					
Google Analytics					
Google Dynamic					
LiveRail					
Lotame					
Mediaplex					
Nielsen					
QuantCast					
Syndication					
Twitter Advertising					

Comparison chart of 3rd party analytics services, red = no use and green = use.
* Blue Kai and Eloqua are Oracle products, Double-Click is a Google Product

Most platforms studied are accessible to Google Analytics and Double-click.net, which can anonymously access Ad Views, Visits, Clicks, Browser Information, Cookies Data, Date/Time, Demographic Data, Hardware/Software Type, Interaction Data, Page Views, Serving Domains. They may also pseudonymously obtain IP Address, Search History, Location Based Data, Device ID, Phone Number and other profile identifiers. When accessed and consolidated toward

unethical ends, these features may reveal more about a user's identity and behavior online than they intended to share. With these trackers and others listed below, data retention is often undisclosed and varies based on company needs.

VI. Conclusions

Social media continues to grow on a daily basis and with their growth the ability to protect their assets, which is often the user, is steadily growing as well. Companies are victims of legitimate system breaches that have led to data leaks, while users have been targets of revealing social engineering techniques. Privacy starts with the user, nearly all companies will allow users to opt out of tracking, start profiles with minimal information, and set settings to only allow vision from those that are trusted. Companies have the ability to do what they want with the agreed upon collected information, as well as the responsibility to prevent harm to the user as a result of information usage. Security breaches are a constant threat to all these networks and while their practices have not always held been the best, improved methods have contributed to increased users totals.

References

https://developers.facebook.com

https://www.instagram.com/developer/

https://developers.google.com/+/web/api/rest/

https://developer.linkedin.com

https://dev.twitter.com

https://blog.twitter.com/2015/sunsetting-sha-1

https://twitter.com/privacy?lang=en

https://support.twitter.com/articles/20169453#

https://support.twitter.com/articles/20170514

http://www.bbc.com/news/business-24397472

http://www.investopedia.com/articles/markets/100215/twitter-vs-facebook-vs-instagram-who-target-audience.asp

https://www.entrust.com/understanding-sha-1-vulnerabilities-ssl-longer-secure/

https://www.theguardian.com/technology/2014/jun/11/twitter-tweetdeck-xss-flaw-users-vulnerable

https://www.theguardian.com/technology/2013/feb/02/twitter-hacked-accounts-reset-security

https://blog.twitter.com/2013/keeping-our-users-secure

https://www.linkedin.com/legal/privacy-policy

https://www.linkedin.com/legal/cookie-policy

https://www.linkedin.com/legal/pop/pop-cookie-table

http://bits.blogs.nytimes.com/2015/02/23/linkedin-settles-class-action-suit-over-weak-password-security/?_r=0

http://thehackernews.com/2014/06/millions-of-linkedin-users-at-risk-of.html

https://www.yahoo.com/tech/this-sneaky-tool-will-let-you-see-anyones-email-on-81301057402.html

https://isis.poly.edu/~jcappos/papers/tr-cse-2013-02.pdf

https://www.ghostery.com/

https://www.semrush.com/

https://www.google.com/trends/explore#q=facebook%20hack%2C%20Twitter%20hack%2C%20LinkedIn%20hack%2C%20Gmail%20hack%2C%20Instagram%20hack&date=3%2F2012%2049m&gprop=news&cmpt=q&tz=Etc%2FGMT%2B5

Appendix:

Facebook:	Company Description	Data
Adobe Marketing Cloud	Provides customers the ability to deliver relevant ads to targeted audiences. Technology provides both data management functionality and a unified campaign management platform that optimizes advertising campaigns across search, display and social.	(Anonymous (Ad views, analytics, Browser Information, Demographic Data, Hardware/Software Type, Interaction Data, Page Views) Pseudonymous (IP Address (EU PII), Search History) Client **Data Retention rate: Undisclosed**
Atlas	Provide Digital Media technologies for agencies, advertisers and publishers. These solutions enable unified management of digital marketing campaigns across display banners, rich media, search, video, and websites.	(Anonymous(Ad views, browser information, Cookie Data, Date/Time, Demographic Data, Hardware/Software Type, Interaction Data, Page Views, Serving Domains) PPseudonymous (IP Address (EU PII), Search History, Clickstream Data) **Data Retention rate: Undisclosed**
Double Click by Google	provides ad management and ad serving solutions to companies that buy, create or sell online advertising.	(Anonymous (Ad Views, Analytics, Browser Information, Cookies Data, Date/Time, Demographic Data, Hadware/Software Type, Interaction Data, Page Views, Serving Domains) Pseduonymous (IP Address (EU PII), Search History, Location Based Data, Device ID (EU PII)) PII(Phone Number) **Data Retention rate: Undisclosed**
Google AdWords	"No matter what your budget, you can display your ads on Google and our advertising network. Pay only if people click your ads."	**Data Collected:** Anonymous (Ad Views, Analytics, Browser Information, Cookie Data , Date/Time, Demographic Data, Hardware/Software Type, Interaction Data , Page Views , Serving Domains) Pseudonymous (IP Address (EU PII), Search History, Location Based Data, Device ID (EU PII)) PII (Phone Number) **Data Sharing:** Anonymous data is shared with 3rd parties. **Data Retention:** Undisclosed
Google Dynamic Remarketing	No matter budget size you can display ads on Google and their advertising network. Only pay if people click on their ads	(Anonymous (Ad Views, Analytics, Browser Information, Cookie Data, Date/Time, Demographic Data, Hardware/Software Type, Interaction Data, Page Views, Serving Domains) Pseudonymous (IP Address (EU PII), Search History, Location Bsaed Data, Device ID (EU PII)) PII (Phone Number) **Data Retention rate: Undisclosed**
LiveRail	Technology solutions that enable and enhance monetization of internet-distributed video.	(Anonymous (Date/Time, Interaction Data, Page Views) Pseudonymous (IP Address (EU PII))

		Data is retained for 3-4 years).
Mediaplex	"Mediaplex provides cross-channel advertising technology solutions and services that enable marketers to achieve one-to-one messaging, greater efficiencies and a competitive edge through insightful reporting and analytics. Our team of industry experts focuses on putting the customer first, providing advanced technology solutions alongside consulting services for the greatest return on their marketing spend."	Anonymous (Ad Views, Browser Information, Date/Time, Hardware/Software Type, Interaction Data , Page Views , Serving Domains) Pseudonymous (IP Address (EU PII), Search History, Clickstream Data) Retention (18-24 months)
Neustar PlatformOne	"A centralized marketing solution, PlatformOne gives you a complete, accurate, real-time portrait of your customer—and enables real-time activation of customer and media intelligence. PlatformOne links customer interactions with authoritative datasets so you can identify, verify and segment customers..."	Anonymous (Browser Information, Cookie Data , Date/Time, Demographic Data, Hardware/Software Type, Interaction Data , Page Views) Pseudonymous (IP Address (EU PII), Clickstream Data) **Data Sharing:** Aggregate data is shared with 3rd parties. **Data Retention:** 12-18 Months Aggregate Knowledge - "We are the world's leading digital data collection company, and uniquely positioned as a true single source solution for any and
		all research projects." **Data Collected:** Undisclosed **Data Sharing:** Undisclosed **Data Retention:** Undisclosed

Google+:		
Tracking Software		
Double Click by Google	provides ad management and ad serving solutions to companies that buy, create or sell online advertising.	(Anonymous (Ad Views, Analytics, Browser Information, Cookies Data, Date/Time, Demographic Data, Hadware/Software Type, Interaction Data, Page Views, Serving Domains) Pseduonymous (IP Address (EU PII), Search History, Location Based Data, Device ID (EU PII)) PII(Phone Number) **Data Retention rate: Undisclosed**