EXHIBIT 125

Google Ads & Data Privacy: Sales Comms

go/adsdatafaq

Confidential: Do not share this document externally

Last Updated June 14, 2018

Objective: This doc is designed to help GBO Googlers understand and communicate Google's approach to user data privacy in ads and respond reactively to customer questions about recent industry events on this topic. We'll update this document in real-time as the situation warrants.

TL;DR: on Google Ads & Data Privacy [Shareable with Customers]

- Google takes a user-first approach in everything we do and our ads products are no different.
- We give users control over their data and transparency over how it is used. Our responsibility is to ensure any data they choose to share is secure.
- We have strict policies about how data can be used to personalize advertising. For example, we do not allow our advertisers to serve ads to people based on sensitive categories (e.g., race, religion, sexual orientation, health conditions, marginalized groups, etc).
- We do not sell your personal information to anyone. We use data to make ads relevant and we show advertisers how well their campaigns worked, but we do not sell personal information like your name, email address, and payment information.
- We are always looking for potential abuses of our systems; if we find any evidence of violations we take action.

Proactive Talking Points:

- Proactive Resource: Google's External Website on Privacy
- Proactive Talking Points: Google's Commitment to Advertising that Works for Everyone

Facebook-Specific [Reactive] Talking Points

- Reactive Talking Points: Facebook and Cambridge Analytica
- Reactive Talking Points: Facebook and Partner Categories
- Reactive Talking Points: Facebook and Custom Audiences [updated]
- Reactive Talking Points: Facebook and Election Security

Related Topics:

- Guidelines: Client Conversations about Audience & Data Solutions **[new]**
- Changes to Doubleclick Data Transfer
- Improving Election Advertising Transparency
- Third Party Ad Serving and Tracking
- How Google fights bad actors

My question isn't answered here, what should I do?

PROACTIVE RESOURCE: Google's external website on privacy

Take a moment to remind customers of all the information already available describing how Google ensures privacy for users, advertisers and publishers in a way that works for everyone.

[Shareable with Customers]

- Our external site - privacy.google.com - outlines our overall commitments to user privacy.
- A section of this site - privacy.google.com/businesses - also outlines how our business partners can control the ways in which their data is used across our platforms. The site also includes regularly updated information on how Google is helping businesses prepare for GDPR (General Data Protection Regulation) with all the services that we provide in Europe. That includes Search and Gmail, and all of our advertising and measurement services like AdWords, AdSense, DoubleClick and Analytics.
- *Googlers only: New to GDPR? Read all about it here and take the training.*

PROACTIVE TALKING POINTS: Advertising that Works for Everyone

On March 21st at Advertising Week Europe, Matt Brittin and Sridhar Ramaswamy reaffirmed Google's continuing commitment to "Better Ads for Everyone" including users, advertisers and publishers.

- Google is committed to working with the ecosystem to ensure advertising works for everyone - first and foremost users, and alongside them for publishers/creators and marketers/agencies. Advertising that works for everyone is valuable, transparent and trustworthy.
- **For users,** making advertising work for them requires security, transparency, and control.
    - First, we ensure all user data is **secure.** If it's not secure, it can't be private.
        - Our engineers work hard to protect people online by developing industry-leading encryption of user searches and properties like Gmail, best-in-class account security with two factor authentication, and automatically updating the security of Chrome.
        - We filter out suspicious emails, block malicious and misleading ads and sites, and alert users if there is any suspicious activity.
    - Once their data is secure, users have **transparency and control** over how it is used.
        - Unique to Google, with **one switch** users can opt out of ads personalisation *across devices*. That is a key feature of Google's My Account, which gives users an overview of their activity data and ability to control whether and how that is used to personalise and improve our services. Only a user can see his or her information, and delete their activity data at any time via My Activity. We never use sensitive information to show ads per our Personalized advertising policy.
        - Tens of millions of users have completed our Privacy Checkup, many of them more than once.

    - We show users how ads are selected for them via Why this Ad, while Mute this Ad allows users to opt out of an ad experience they don't like. We recently announced that Mute this Ad now works across devices when logged-in — any ad you mute on your phone also won't show up on your laptop. Mute this Ad now also works across Doubleclick, so users have more control of the ads they see on more sites and apps than ever before. We also recently launched the ability for users to mute Reminder Ads in apps and on websites that work with Google to show ads.
    - If users would like to download their data from Google and use it with a different service, they can with Download Your Data (formerly Takeout) which has been available since 2011.
- *Googlers Only: Watch Matt & Sridhar's talk at Advertising Week Europe here, and read all the customer facing comms on the "Advertising for Everyone" initiative here.*

GUIDELINES: Sales Conversations about Audience & Data Solutions

Context [Do Not Share Externally]
Given the ever-changing press climate and industry discussions on privacy and the use of data in marketing, we need to be even more conscientious about how we communicate our product solutions in the market.

These guidelines are intended to help you navigate sensitive topics and help guide the creation of collateral -- slides, one-sheeters -- that is shared with advertisers or agencies. Understanding that we cannot centralize review of all materials, we want to provide clear guidelines to help you frame Google's solutions in a thoughtful way, given today's climate. (*For guidance on 1:many marketing communications, please review Principles for Marketing on Sensitive Topics through Marketing channels.*)

Reminder on our Principles [Do Not Share Externally]

- **Respect the user.** Ensure our content builds trust.
    - Highlight the user benefit, and when possible, take a user-centric view of what we provide from an ads and platforms perspective. Google builds great experiences and creates user value with the "consent" of users. Highlight user choice and transparency, whether that applies to consumer control of data or advertiser controls.
    - Highlight our commitment to trust and responsibility for/with advertisers and publishers. Our platforms and ads products support our beliefs as a company.

- **Respect the opportunity.** Think like an owner and prepare for all the possibilities -- including a skeptical member of the press looking for a scoop.
- **Context and audience are critical.** Apply the right lens for content published in open, public forums or more private, professional settings with customers.
- **Step back, pause.** The environment has changed/is changing. Does yesterday's world apply today? Are we prepared for tomorrow? Check it once. Check it twice. Check again.

Guidelines for Client Conversation on Audience & Data Solutions [Do Not Share Externally]

Below we've outlined situations where we recommend modifying language or adding slides to underscore Google's commitment to privacy. The intent is not to go into archived content and do a complete overhaul, but rather to guide content made from this point forward. That said, if you are aware of particularly problematic items, it is strongly recommended that you update materials covering sensitive topics or consider deprecation for content that's no longer relevant or needed.

Situation	Recommendation
In the past, your sales collateral has used language like **"Target** users" or "**Targeting**" (i.e. of people, users, audiences, consumers), including variations of those words or related terms like **"track"**	Try to use language like: "Find users," "Reach users," "Engage users" "show ads to users" or "make ads more relevant" or "deliver relevant ads"
You're presenting slides that outline Google's audience solutions (e.g. In-market, Affinities, Customer Match).	• Consider adding this small note at the bottom of slides that reference audience solutions: ○ *Note: Will not apply to people who've chosen not to see personalized ads* (seen here) • Consider adding this slide to your presentation, outlining Google's commitment to privacy & transparency • Consider adding this slide for EEU customers
You are asked to print or email a leave-behind version of a presentation that provides details on Google's audience solutions (e.g. decks like this audience story)	**ONLY** share leave-behind copies with customers under NDA, and do so sparingly if possible. (e.g. don't share unless a client asks and/or it's critical to business relationship)
You're asked to share Google's POV on data and/or privacy	See below section on Better Ads Ecosystem narrative

REACTIVE TALKING POINTS: Facebook and Cambridge Analytica

Context: *On Saturday, March 17, The New York Times and The Guardian reported that Cambridge Analytica and parent company SCL illegitimately obtained private data of 50 million Facebook users. Facebook pre-empted the news by announcing they'd be banning CA and SCL from their platform for violating their policies. In order to get more voter profile data, targeting firm Cambridge Analytica partnered with an academic who created a Facebook app (a personality quiz) that ultimately scraped data from people who installed it (about 270K) as well as their friends (est. 50M total), which was then shared with CA to combine with other data sources to build detailed psychographic profiles. FB was reportedly made aware of this in 2015 and made efforts to secure the data, although NYT and Guardian reported that CA still has it.*

Please use this reactive verbal-only statement as our main message (do not use this as an opportunity to pitch competitively against FB):

- "We have always been and always will be focused on the privacy and security of our users. We've seen no indication of this type of abuse on our platforms. We have policies that prohibit deceptive behavior and misuse of personal data. If we find evidence of violations we will take action."

Additional reactive verbal-only talking points on Facebook and Cambridge Analytica (again, do not use this as an opportunity to pitch competitively against FB):

- We've seen no indication of this type of abuse on our platforms. We have policies that prohibit deceptive behavior and misuse of personal data.
- The Google API policy prohibits deceptive practices like misrepresenting how data is being used or the entity using the data. It also prohibits aggregating and reselling the data to third parties.
- We have policies that disallow apps in Google Play that are deceptive or misuse personal data.
- We also have ads policies that prohibit misusing personal information.
- We are always looking for potential abuses of our systems; if we find any evidence of violations we will take action.

REACTIVE TALKING POINTS: Facebook and Partner Categories

Context: *On Wednesday, March 28, several news outlets reported that Facebook is shutting down Partner Categories, a product that enables third-party data providers like Experian and Acxiom to offer their targeting directly in Facebook. Graham Mudd, a product marketing director at the company, gave a statement: "While this is a common industry practice, we believe this step, winding down over the next six months, will help improve people's privacy on Facebook."*

Reactive verbal-only talking points on Facebook and Partner Categories (do not use this as an opportunity to pitch competitively against FB):

- We have never allowed third-party data for targeting on Search and Gmail. And In January 2017 we announced changes to YouTube, including deprecating support for targeting using anonymous third-party cookies.
- DoubleClick Bid Manager, unlike AdWords, is a customizable platform that enables advertisers to license third-party data from integrated data providers. All these providers are vetted before integrating with our platform and are subject to policies that prohibit targeting based on sensitive information. Third-party data may be used for targeting by an advertiser on DBM or via an AdX buyer. Google does not use this information to build or augment our profiles used for ads personalization.
- *[Please only reference if specifically asked about this beta]* Over the last few years, we experimented with a small beta program with third-party data providers on the Google Display Network. In February 2018, we made the decision to wind this down, and it will be fully discontinued in April 2018.
- Customer Match on AdWords, which has launched for Search, YouTube, and Gmail campaigns, has its own dedicated policy which states that advertisers can only upload customer information that was collected in a first-party context -- i.e. collected directly from the user by the advertiser.
- **Q: What about Facebook Custom Audiences? A:** *Marketers can still use third-party data audiences via Facebook Custom Audiences, but this requires a marketer to form a direct relationship with the data provider vs. accessing the data directly in Facebook's UI. Customer Match (our Custom Audiences equivalent) does not allow any third-party audience lists.*

REACTIVE TALKING POINTS: Facebook Custom Audiences Workflow Change

On June 13, Facebook posted several changes to their Custom Audiences workflow. Advertisers must now specify the data origin (directly from customers, directly from partners, customers and data partners), accept an audience-sharing relationship through Business Manager for shared lists (e.g., a marketer sharing a list with an agency to upload), and accept Custom Audiences terms for every user uploading a list, not just the admin on the account. Facebook users will also be provided with more information on why they are seeing a Custom Audiences ad --- the advertiser name and ID that was uploaded (phone number, email address, device ID).

Reactive, verbal-only talking points:

- Both Google and Facebook have policies regarding data uploaded for use in Customer Match and Custom Audiences, respectively.
- Google Customer Match:
    - Google's policy states that advertisers may only upload customer information that they collected in a first-party context—i.e., information they collected from their own websites, apps, physical stores, or other situations where customers shared their information directly. Unlike Facebook, Google does not allow [third-party] partner data to be uploaded via Customer Match.
    - We require that advertisers confirm adherence with our Customer Match policies as part of campaign workflows in AdWords.
    - We do not allow Customer Match lists to be shared between entities.
    - We show users why they are seeing Customer Match ads via "Why this ad," and allow users to mute ads they no longer want to see.
- Facebook Custom Audiences:
    - Facebook allows both first-party (customer) lists and third-party (partner) lists to be uploaded via Custom Audiences. The new requirement to specify "origin of data" stems from a willingness to enable third-party data.
    - Facebook allows list sharing between entities, hence the new requirement for an audience-sharing agreement to be signed by both parties.
    - Facebook is requiring Custom Audiences terms to be accepted by each user; Google has always required our Customer Match terms to be accepted directly in the campaign set-up flow.
    - Facebook has now incorporated Customer Match targeting criteria into their version of "Why this Ad" - Google offers similar transparency.
- *Googlers only: Screenshots of AdWords Customer Match and Facebook Custom Audiences upload pages (as of 3/31/18):*

REACTIVE TALKING POINTS: Facebook's Election Security Update

On Thursday, March 29th Facebook announced a series of updates on their steps to protect elections from abuse and exploitation on their platform. For elections advertising, Facebook will require authorization of US advertisers placing political ads (by submitting government-issued IDs and a physical mailing address in the US), requiring in-ad "paid for by" disclaimers for political ads, and launching a public archive showing all ads that ran with a political label. This was followed-up by a post from Mark Zuckerberg on Apri 6th.

Reactive, verbal-only talking points:

- Google is taking steps to safeguard our platform for lawful US political advertising. We announced several initiatives in a blog post on October 2017; all of these efforts are on track for completion this spring and summer.
- U.S. law restricts entities outside the U.S. from running election-related ads. We'll reinforce our existing protections by requiring that advertisers proactively identify who they are and where they are based before running any election-related ads. As they do, we'll verify that they are permitted to run U.S. election campaigns through our own checks.
- Only verified advertisers will be able to use Google political audiences (election-specific Affinity segments, In-Market segments).
- We'll identify the names of advertisers running election-related AdWords campaigns through an in-ad disclosure.
- In 2018, we will release a transparency report for election ads to share data about who is buying election-related ads on our platform and how much money is being spent.
- We'll also introduce a publicly accessible database of election ads purchased on AdWords and YouTube with information about who bought each ad.

RELATED TOPIC: Changes to Doubleclick Data Transfer

As part of our ongoing commitment to user privacy, on April 27th we notified customers that we are making important changes to our DoubleClick data transfer feature, starting May 25th to align with GDPR:

Shareable talking points on the changes:

- YouTube: We will stop populating the encrypted UserID and PartnerID fields in data transfer for impressions served on YouTube inventory globally and recorded in DoubleClick Campaign Manager and DoubleClick Bid Manager.
- DoubleClick Digital Marketing: We will stop populating encrypted UserID and PartnerID fields in data transfer for events associated with EEA users recorded in DoubleClick Campaign Manager and DoubleClick Bid Manager. We intend to apply these changes globally, and will announce timing for non-EEA countries later this year.
- DoubleClick Ad Exchange: We will remove encrypted cookie IDs and list names (if used) from the data transfer file for all global bid requests to Ad Exchange buyers.

Reactive, verbal-only talking points:

- Google takes a user-first approach in everything we do. We never sell users' personal information, and tools like My Account, Why this Ad and Mute this Ad give users transparency and control over their ad experiences. This user-first approach also applies to our ads reporting. We already encrypt and anonymize user information in features like DoubleClick's data transfer, while still providing advertisers the power to deliver more relevant ads and measure their impact.
- We recognise these changes may be disruptive to you and the systems that power your digital marketing. Ad reporting is an important part of the digital ecosystem, providing efficiency for agencies and marketers, and we are committed to partnering with you to help refine strategies to effectively use and manage data based on these changes. We are investing heavily in the expansion of Ads Data Hub and providing alternative solutions and services for many key use cases such as custom attribution, audience management, media optimisation, and offline-to-online.
- We continually evaluate our data and privacy practices. In consideration of the implications to our users, advertisers and publishers, it recently became clear that the appropriate approach to handling the UserID and PartnerID fields in data transfer feature was to zero them out completely. Reaching this decision was not taken lightly and we considered multiple alternatives before going

forward with this approach. We believe that taking this approach, and aligning the change with GDPR - which takes effect May 25th - is in the best interest of our customers and partners.

Googlers only: Need more on this change? Read all about it here.

RELATED TOPIC: Improving Election Advertising Transparency

On May 4th, Google announced new policies for U.S. election ads across our platforms, as part of our commitment to make political advertising more transparent.

Reactive talking points [OK to share in writing, or refer to the blog post.

- Google will now require additional verification for anyone who wants to purchase an election ad in the U.S. and require that advertisers confirm they are a U.S. citizen or lawful permanent residents, as required by law. That means advertisers will have to provide a government-issued ID and other key information. To help people better understand who is paying for an election ad, we're also requiring that every ad incorporate a clear disclosure of who is paying for it.
- This summer, we'll also release a new Transparency Report specifically focused on election ads. This report will describe who is buying election-related ads on our platforms and how much money is being spent. We're also building a searchable library for election ads, where anyone can find which election ads ran on Google and who paid for them.
- As we learn from these changes and our continued engagement with leaders and experts in the field, we'll work to improve transparency of political issue ads and expand our coverage to a wider range of elections.

Googlers only: Need more? Visit this FAQ

RELATED TOPIC: Google third-party ad serving and tracking

In addition to giving users security, transparency and control over how their data is used by Google products, we also take our role very seriously as a steward of user data when partnering with third-party ad serving and measurement companies. You may be receiving questions about how Google works with 3rd parties to serve or track advertising placements.

Reactive verbal-only talking points on 3rd party ad serving (3PAS) and tracking (3PAT):

- Google Adwords has a rigorous, human-led certification process for third-party partners that can serve or measure ads on AdWords, YouTube, and DoubleClick Ad Exchange.
- Google Adwords has ads policies related to third-party ad serving and measurement that prohibit impression-level tracking for ads personalization.
- In addition to our own measurement options, we will allow a limited number of certified third party vendors - including comScore, DoubleVerify, IAS, MOAT, Nielsen, Kantar, and Research Now - that meet our technical and privacy requirements to measure on YouTube.
- With our Doubleclick data transfer solutions, we do not pass a user's Doubleclick ID for several privacy reasons, including when ad campaigns are served based on Google user interests.
- We are actively investing in Cloud-based measurement solutions like Ads Data Hub, launched last year. Built on infrastructure from Google Cloud, including BigQuery, Ads Data Hub gives advertisers or their preferred measurement partners access to detailed, impression-level data

about their media campaigns across devices in a secure, privacy-safe environment. Consistent with our commitment to privacy, no user-level data can be removed from the secure Cloud environment.
- *Googlers only: Want more on 3PAS/T? Read all about it here.*

RELATED TOPIC: How Google fights bad actors

The advertising industry has a long history of bad actors looking to profit from invalid traffic, ad fraud, misrepresentative content and more. Google takes its role very seriously in combating bad actors by constantly making improvements to protect the integrity of our systems and our users' security.

Reactive verbal-only talking points on fighting bad actors:
- In March 2018, we released highlights from 2017 with stats about how we protect our advertisers, publishers and users from bad actors in this blog post. For example, we removed 100 bad ads per second in 2017, 320,000 publishers and more. We followed this quickly with more details on how this works in practice on our ad network.
- In March 2018, we shared that we've trained our systems so that during breaking news events, we adjust our signals more towards authoritative content, working to reduce the likelihood people will be exposed to inaccurate content as they search for information (blog post)
- In March 2018, as part of our Google News Initiative, we announced that we're launching a Disinfo Lab alongside First Draft in order to combat misinformation during elections and breaking news moments (blog post)
- In September 2017 Doubleclick announced its plans to work with the industry towards a fraud-free media supply chain, including reducing the ability for bad actors to profit from fraud and adoption of the ads.txt standard to increase supply chain transparency and make it more difficult to sell counterfeit inventory.
- We were concerned about 'fake news,' low quality and offensive results turning up in search, so we launched "Project Owl", announced in April 2017 to improve our ranking signals
- In November 2016 we were concerned about sites misrepresenting themselves as news sites abusing our ads systems, so we introduced a new misrepresentative content policy for AdSense and have since taken action against hundreds of publishers in violation.
- In 2016 we also introduced the Fact Check Label to provide useful context for people as they explore information online, which is now available globally in search and Google News.
- *Googlers only: Want more on Ads Traffic Quality? Read all about it here.*

My question isn't answered here. What should I do?

1. Check back often, we'll be updating this document in real-time as necessary.
2. If you have a burning question that you think needs to be included in our FAQ, please email adsdatafaq@google.com and we'll either add it or direct you to resources that could help.
3. Contact your regional sales Go-to-Market lead as listed below:
    - EMEA LCS: Carl Fernandes, Nicola Roviaro
    - AMER LCS: Owen Jones
    - APAC LCS: Anne Ascharsobi
    - GCAS: Guillaume Schmidt
    - GMS: Francisco Elizondo

- Global Product Experts: Julia Weinberg, David Bledin