An e-White Paper:

A Case Study of Alphabet-Google's 2004-2018 Privacy Track Record of Evident Unfair and Deceptive Over-collection of Consumers' Personal Data Exposes an Evident Gap in the FTC's Remedial Authority to Protect Consumers

Submitted as a public comment for the FTC's fall 2018
"*Competition and Consumer Protection in the 21st Century Hearings.*"
Topic #5: *"The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters"*
FTC Project Number: P181201

July 30, 2018

By Scott Cleland
President, Precursor® LLC info@precursor.com & Chairman, NetCompetition®

Disclosures: *These public comments are my own. No one requested these public comments be submitted or has reviewed them prior to publication. I am Scott Cleland* and *served as Deputy U.S. Coordinator for International Communications & Information Policy in the George H. W. Bush Administration. I am President of Precursor LLC, an internetization consultancy specializing in how the Internet affects competition, markets, the economy, and policy, for Fortune 500 companies, some of which are Internet platform competitors. I am also Chairman of NetCompetition, a pro-competition e-forum supported by broadband interests. I have testified seven times before the Senate and House Antitrust Subcommittees on antitrust matters, twice before House Subcommittees on Privacy, and overall, eight different congressional subcommittees have sought my expert testimony a total of sixteen times. When I served as an investment analyst, Institutional Investor twice ranked me the #1 independent analyst in communications.*

I. Conclusion

This case study of Alphabet-Google's track record of unfair and deceptive privacy and data security practices provides a compelling body of evidence of 17 major business practice examples over a fifteen-year period that indicate the FTC evidently does not have enough remedial enforcement authority to deter Google, or other Internet platforms, from engaging in unfair and deceptive conduct in privacy and data security matters.

It is also evident from Google's words and actions chronicled below that it legally does not believe its users have a "legitimate expectation of privacy" concerning the information they provide to Google.

Given that the FTC understands deterrence is inherently a causal concept, and given the evidence provided in this e-white-paper, it is reasonable for the FTC to conclude that its admitted lack of FTC remedial enforcement authority for privacy and data security is in part causing the evident effect of Google's rampant recidivism on privacy and data security matters.

The cumulative evidence chronicled in this Google case study exposes that the FTC has not deterred Google from serial unfair and deceptive practices via multiple services, involving multiple technologies, in multiple ways, repeatedly, over a fifteen-year period.

The evident common causal thread is Google's business modus operandi of unfair and deceptive over-collection of private information by default.

Google has serially harmed consumer welfare in unfairly and deceptively undermining consumers' expectation of, and actual, privacy and data security, as well as undermining consumers' ability to protect their own privacy and data security and that of minors.

A big question for the FTC's congressional overseers and the FTC to ask in the Simons hearings this fall, is why Google has been able to serially, unfairly, and deceptively violate consumers' reasonable expectation of privacy repeatedly, in many dimensions, for 15 years with evident impunity?

Is this systemic risk and failure just a result of insufficient FTC "*remedial authority to deter unfair and deceptive conduct in privacy and data security matters?*"

Or is it also partially a result of: 1) the FTC's legal case-specific lens, processes, and procedures that may be failing to see the big picture and systemic patterns of bad practices over time or across services; 2) Google and other platforms' Section 230's exemption from Federal regulation and immunity from civil liability; and/or 3) regulatory capture?

Bottom-line: The FTC badly needs additional privacy and data security authority from Congress to deter the rampant recidivist unfair and deceptive privacy and data security practices of Google, and other Internet platforms.

II. Summary of the FTC-Google Privacy Case Study

This case study of Alphabet-Google's track record of unfair and deceptive privacy and data security practices is empirical research that spotlights the causal relationship between the FTC's evident lack of remedial privacy and data security authority and Google's evident privacy and data security recidivism.

It also provides research in support for FTC Chairman Simons' recent testimony before Congress where he stated the FTC needs more privacy and data security authority from Congress.

> Chairman Simons testified: *"The Commission continues to reiterate its longstanding bipartisan call for comprehensive data security legislation." "Section 5 does not provide for civil penalties, reducing the Commission's deterrent capability. The Commission also lacks authority over non-profits and over common carrier activity, even though these acts or practices often have serious implications for consumer privacy and data security. Finally, the FTC lacks broad APA rulemaking authority for privacy and data security generally."*

If the FTC had enough privacy and data security deterrent authority, it is reasonable to expect that after the 2011 FTC-Google-Buzz 20-year privacy decree, that Google would stop, or at least curtail, its

unfair and deceptive practices going forward, not the exact opposite, serially repeating them at least *nine* times subsequently with apparent impunity.

Apparently, Google has little reason to fear the FTC on these matters.

First, from 2004 to 2018 Google has established an evident, serial recidivist track record of unfairly, deceptively, and systemically intercepting and misusing personal communications that consumers reasonably expect are private.

Seven of the most evident examples chronicled below are:

2004 -- Google scanning personal Gmail exchanges to serve ads without others' knowledge or consent;

2010 – Google-Street View's undisclosed secret mass-eavesdropping of home WiFi communications;

2013 – Google Glass enabling recording of conversations without others' knowledge or consent;

2015 – Google Chrome eavesdropping tool installed on computers without knowledge or consent;

2015 – Google-Nest-Aware eavesdropping on home conversations without others consent.

2017 – Google Home Mini designed to secretly record conversations without knowledge or consent; and

2017 – Google-Android secretly records all device locations even if user disables all location services.

This is not accidental, one-off, or anecdotal. This is evidence of a lasting, purposeful, modus operandi of designing new products and services that by default unfairly, deceptively, and systemically intercept, over-collect, and misuse personal communications that consumers have a reasonable expectation are private.

Second, from 2011 to 2018 Google has established an evident unfair and deceptive consumer privacy modus operandi and track record of bait-and-switch, promising and representing to the public one thing and apparently knowingly and repeatedly doing the opposite.

Ten of the most evident examples chronicled below are:

2011 – Google Buzz social network did not give users the privacy control they represented;

2012 – Google completely changed its privacy policy for Google+ without users' affirmative consent;

2012 – Google hacked Safari browser to track Apple's users and serve them ads without consent;

2013 – Google Play shared personal info with app developers without user knowledge/consent;

2013 – Google Wallet shared users' personal info with app developers without user knowledge/consent;

2014 – Google+ forced users to publicly associate with people they do not know without their consent;

2015 – Google Education made the Student Privacy Pledge, but does not abide by its representations;

2016 – Google-DoubleClick combined personal info and ad tracking data after promising it would not;

2017 – Google secretly tracked users in-store purchase activity without user knowledge/consent; and

2018 – Google-YouTube uses minors' personal info without required parental knowledge/consent.

III. The Evidence of Google's MO of Unfair/Deceptive Privacy and Data Security Practices

A. From 2004 to 2018 Google has established an evident, serial recidivist track record of unfairly, deceptively, and systemically intercepting and misusing personal communications that consumers reasonably expect are private.

1. 2004 Google Gmail

In 2004, Google begins scanning Gmail to serve ads; in 2013 Federal court rules the practice is wiretapping; and in 2017 Google claims to stop wiretapping.

In April 2004, after Google announced that it would begin scanning confidential emails for content to serve ads, the World Privacy forum and 30 other privacy organizations wrote a letter to Google asking them to suspend the practice because they did not get consent from the scanned emailers and because of "*the dangers of lowered expectations of privacy in the email medium*."

Eventually in 2013, a court ruled that Google could be sued for illegal wiretapping for scanning confidential emails. Legal discovery in a Gmail privacy class action suit, Fread v. Google, uncovered a secret Google network device called "*Content One Box*" that enabled Google to secretly intercept and wiretap, literally hundreds of millions of peoples' emails from at least 2009-2013.

The presiding Federal judge in the case, Judge Lucy Koh, ruled that Google's scanning of Gmail exchanges to create personal advertising profiles constituted wiretapping. Specifically, Judge Koh ruled that Google's reading of people's email is not an "*ordinary course of business*" and that "*accepting Google's theory of implied consent… would eviscerate the* [wiretap] *rule against interception*." The Ninth Circuit Court of Appeals unanimously affirmed Judge Koh's wiretapping decision.

This Google wiretapping was unfair and deceptive because it was a secret not known to the public.

Bloomberg's Joel Rosenblatt reported this courtroom exchange: There is *"…a device Google has used to intercept e-mails called the "content one box." Google determined that the device couldn't extract information from e-mails that weren't opened or deleted, or when they were accessed by phones or through Outlook, Rommel said. In 2010, Google moved the device from the storage end of e-mail services to the "delivery pipeline" to extract data before users receive the messages, Rommel said. "That's the secret," Rommel said. "It is factually inaccurate to say that the location and the timing of that interception is in the public record," he said, referring to Google's disclosures about its scanning. "There is not a single disclosure in the record that identifies, alerts, tells anybody that there is an interception occurring. It's not there, it doesn't exist*."

In defending itself before the Ninth Circuit Court of Appeals in 2013 Google said users do not have a legitimate expectation of privacy when using its services like Gmail. ***"Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their emails are processed by the recipient's [email provider] in the course of delivery. Indeed, 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'"*** [Bold added for emphasis.] (Motion to dismiss, Page 19)

In June 2017, Google announced it would stop scanning Gmail confidential emails for advertising purposes, after thirteen years of proactively, systemically, and deceptively forcing a lowering consumer expectation of email privacy as Gmail went on to become the world's leading email provider with over 1.4b users.

Gmail isn't the only service Google introduced unfairly and deceptively, and that apparently were other forms of illegal wiretapping.

2. 2010 Google Street View Wiretapping

Google Street View's deceptive systemic WiFi Data Collection from 2008-2011 was affirmed legally as wiretapping in 2014 by the U.S. Ninth Circuit Court of Appeals.

A few thousand Google Street View vehicles were caught collecting unauthorized WiFi communications from tens of millions of homes in over thirty countries. Google was sued for breaking federal laws by secretly collecting people's email, passwords and other personal information as part of its Street View mapping project, which began in 2007.

In fighting this Google Street View class action suit in the U.S., Google appealed to the U.S. Supreme Court that its unauthorized interception of home WiFi signals was not wiretapping, but Google ultimately lost that argument when the Supreme Court denied hearing Google's appeal. Evidently, Google systemically illegally wiretapped millions of American's WiFi communications.

Interestingly in 2010, the FTC investigated and dropped its inquiry with no action. In 2013, 38 State Attorneys General fined Google $7m fine for its illegal and deceptive collection of consumers WiFi data via its StreetView process.

3. 2013 Google Glass Wiretapping?

Google "Glass" evidently was designed to deceptively wiretap users' conversations.

In 2013-14 Google Glass was enabled with an always-on audio receiver to listen for the audio command "OK Google," and since Glass could video and audio record one's surroundings with a finger tap or a voice command, Google Glass could record people's private conversations without their knowledge or consent. Tellingly, CIO.com advised that Google Glass' "Secret Video and Audio Recordings [are] a Legal Minefield for Employers."

4. 2015 Google Chrome Wiretapping?

Google Chrome evidently was designed to deceptively wiretap users' conversations.

A 2015 Guardian article, "*Google eavesdropping tool installed on computers without permission*," reported: "*Privacy campaigners and open source developers are up in arms over the secret installing of Google software which is capable of listening in on conversations held in front of a computer*." See this Rick Falkvinge post for more detail. Tellingly, this is not the first time Google Chrome's wiretapping

ability by design was uncovered. In 2014, Gizmodo reported that Google's Chrome browser had a way for any website to listen to a website-visitor's computer microphone, even after the user closed the website link.

5. 2015 Google Nest Wiretapping?

Google "Nest-Aware" evidently was designed to deceptively eavesdrop on users' conversations.

A separate 2015 Guardian article entitled, "Google's *new Nest Cam is always watching*, *if you let it into your home*," reported: "*With Nest Aware, Google is also offering to record up to 30 days of video, with audio, to the cloud and do constant analysis of it*." The purchaser of the Nestcam service may approve of the Google audio recordings, but recorded visitors have not.

6. 2017 Google Home Mini Wiretapping?

When Google released its new Home Mini speaker device to reviewers, the reviewer at Android Police, Artem Russakovskii discovered "*that his device was turning on by itself , recording his conversations, and uploading them to Google*" all without his knowledge or consent, per Business Insider.

This is additional evidence that Google believes its users have no legal legitimate expectation of privacy and that they can unfairly and deceptively design their new products and services to wiretap or over-collect private conversations without people's knowledge or consent, and with impunity.

7. Google-Android's Secret Location Tracking

Google's Android operating system and location services deceptively and systemically over-collect users' locations even when users try every available effort to not be tracked.

A 2017 Quartz investigation of Android and Bluetooth determined that Google-Android devices collect a wide variety of location information automatically without permission and have made it deceptively hard to fully turn off any Google tracking. This apparently is an unreasonable violation of a user's expectation of privacy.

The House Committee letter to Alphabet CEO Larry Page said: "*Android users have a reasonable expectation of privacy when taking active steps to prevent being tracked by their device*.

Just this June 2018, the U.S. Supreme Court, decided in *Carpenter v. United States* that Americans still enjoy a Constitutional right to privacy in the mobile Internet world and era, in ruling that U.S. law enforcement must get a probable cause warrant to examine a citizen's location and movement history stored in their smartphone. Specifically, relevant to the wanton overcollection of users' comprehensive location histories, the Supreme Court's Carpenter decision tellingly said: "*A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements*."

Apparently, the FTC has been a non-factor in deterring these evident serial unfair and deceptive privacy and data security practices.

B. From 2011 to 2018 Google has established an evident unfair and deceptive consumer privacy modus operandi and track record of bait-and-switch, promising and representing to the public one thing and apparently knowingly and repeatedly doing the opposite.

1. 2011 Google-Buzz

In a seminal 2011 FTC-Google privacy settlement that was supposed to be the FTC template for deterring privacy and data security abuses by Internet platforms, the FTC charged Google with "*deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010. The agency alleges the practices violate the FTC Act. The proposed settlement bars the company from future privacy misrepresentations, requires it to implement a comprehensive privacy program, and calls for regular, independent privacy audits for the next 20 years.*"

The FTC's announcement of charges against Google explained the unfair and deceptive practices.

> "*According to the FTC complaint, Google launched its Buzz social network through its Gmail web-based email product. Although Google led Gmail users to believe that they could choose whether or not they wanted to join the network, the options for declining or leaving the social network were ineffective. For users who joined the Buzz network, the controls for limiting the sharing of their personal information were confusing and difficult to find, the agency alleged.*
>
> *On the day Buzz was launched, Gmail users got a message announcing the new service and were given two options: "Sweet! Check out Buzz," and "Nah, go to my inbox." However, the FTC complaint alleged that some Gmail users who clicked on "Nah..." were nonetheless enrolled in certain features of the Google Buzz social network. For those Gmail users who clicked on "Sweet!," the FTC alleges that they were not adequately informed that the identity of individuals they emailed most frequently would be made public by default. Google also offered a "Turn Off Buzz" option that did not fully remove the user from the social network*."

2. 2012 Google+ New Privacy Policy

Moreover, just two months after the FTC finalized the FTC-Google-Buzz new privacy framework that required Google to allow consumers to opt-out of privacy policy changes, Google announced the biggest changes to its privacy policy ever to allow its social network, Google+, to combine the privacy policies of different products into one overall privacy policy.

However, Google evidently did so without respecting the new critical FTC requirement that Google allow users to opt out of changes in privacy policy, i.e. "*Obtain express affirmative consent from the Google user to such sharing*" of the users personal information.

The FTC apparently did not take enforcement action on Google+'s apparent violation of the new FTC-Google-Buzz privacy decree, despite coincidently working on its biggest consumer privacy report at the time entitled, "*FTC Privacy Report: Balancing Privacy and Innovation*."

However, thirty-six State Attorneys General did object to the new privacy policy without an user opt-out and tellingly new Google CEO Larry Page refused to meet with the State Attorneys General on the matter. Google CEO Larry Page also refused EU privacy regulators request to delay introduction of the new privacy policy to see if it violated EU privacy laws requiring consumer opt-out.

Tellingly coincident with Google's apparent Google+ privacy decree violation, the FTC did ask Congress for more privacy and data security authority. In testimony before Congress, then FTC Chairman Leibowitz said:

> "*Just last month, the Administration released its final "White Paper" on consumer privacy, recommending that Congress enact legislation to implement a Consumer Privacy Bill of Rights. Today we recommend that Congress consider enacting general privacy legislation. We reiterate our call on Congress to enact legislation requiring companies to implement reasonable security measures and to notify consumers in the event of certain security breaches, as well targeted legislation that would provide consumers with access to information about them held by data brokers."*

3. Google Hack of Safari Browser

Less than a year after agreeing to the FTC-Google-Buzz enforcement decree in 2012, Google violated the FTC-Google-Buzz consent decree.

The FTC announced:

> "*Google Inc. has agreed to pay a record $22.5 million civil penalty to settle Federal Trade Commission charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC. The settlement is part of the FTC's ongoing efforts to make sure companies live up to the privacy promises they make to consumers, and is the largest penalty the agency has ever obtained for a violation of a Commission order. …"*
>
> *"The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order," said Jon Leibowitz, Chairman of the FTC. "No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place*."

The FTC's decree, in which Google did not have to admit that it violated any law and had to pay a record $22.5m fine, evidently did not deter Google from breaking its promises to consumers. In 2013, Google also paid a $17m fine to 37 State Attorneys General for the same Google Safari hack violating Google's privacy misrepresentations to consumers.

4. 2013 Google Play

In February 2013, one month after the FTC abruptly closed all of its antitrust probes into Google, Consumer Watchdog asked in a letter to the FTC calling for the FTC to act immediately to enforce the FTC-Google-Buzz privacy decree for Google's most recent privacy violation – sharing users' personal information with Android App Store apps developers – and said the penalties for violating a previous consent order should reach into the billions of dollars, given the record $22.5m fine in August of 2012 for Google violating so-called "Buzz Consent Order" again.

5. 2013 Google Wallet

In April 2013, three months after the FTC abruptly closed all of its antitrust probes into Google, the FTC apparently looked the other way and did not sanction Google with a fine for de facto admitting they violated the FTC-Google-Buzz Privacy consent decree by stopping the offending privacy violation of sending Google Wallet users' personal information to app developers via Google Play without their knowledge or meaningful consent. Consumer Watchdog's blog post is here; Consumer Watchdog's complaint is here; and Representative Hank Johnson's letter to the FTC asking for answers is here.

6. 2014 Google+ Forced Association

In January 2014, Consumer Watchdog files complaint that Google+ violates FTC-Google-Buzz consent decree: Consumer Watchdog's complaint explained:

> "*…a newly announced "feature" that would allow people to send emails to Gmail accounts without knowing their email address, violates the "Buzz" Consent agreement. First, Consumer Watchdog urges you to take immediate action to halt the unfair practice, which allows people to be forced to be associated with people with whom they do not wish to be connected. Second, we call on you to block Google's announced plan to open Gmail users' inboxes to anyone on the Google+ social network. … To understand the unfair practice that violates Section 5 it is necessary to compare Google+ with other social networks such as Facebook. In Facebook for example, a person receiving a request from an individual to be their "friend" must approve that request. If the person chooses not to accept, he or she is in no way associated with the individual. On Google+ any individual can add a user to his "Circles." If the user does not appreciate the posts he receives from them, they can block the individual. However, if anyone visits the person's profile and he has opted to display publicly who is in his Circles, the user's name and picture will still appear there. The second user cannot remove himself from the first user's Circles, no matter what, once that person has placed them in their Circles. A user can be forced to be publicly associated with someone with whom they do not wish to be associated. This is a fundamental privacy flaw and must be fixed. People must have the right to choose with whom they are associated*."

This Google practice is eerily like the FTC problems with the Google Buzz launch.

> "*According to the* [2011] *FTC*-[Google-Buzz] *complaint, Google launched its Buzz social network through its Gmail web-based email product. Although Google led Gmail users to believe that they could choose whether or not they wanted to join the network, the options for declining or leaving the*

social network were ineffective. For users who joined the Buzz network, the controls for limiting the sharing of their personal information were confusing and difficult to find, the agency alleged.

Tellingly, Google engaged in largely the same coercive, unfair and deceptive practice with its Google+ social network that it did with its Google-Buzz social network.

7. 2015 Google Education and Student Privacy Pledge

Google publicly committed to the "Student Privacy Pledge" but it apparently does not respect it and the FTC apparently does not enforce it.

January 22, 2015, Precursorblog catalogued evidence of Google's public commitment to the Student Privacy Pledge: "Google quietly signed the U.S. Student Privacy Pledge, which makes its new privacy representations legally enforceable by the FTC and State Attorneys General. …

Importantly, Google initially chose not to sign the Student Privacy Pledge with the original 75 companies that did. It only signed under brand duress after President Obama announced at the FTC that his Administration would "*make sure that those schools and those parents know*" which companies have not signed the Student Privacy Pledge. Uncharacteristically, Google signed the pledge without any public relations announcement. Importantly, when Google was asked by the WSJ about its signing of the pledge, a Google spokeswoman said: "*We've signed the pledge to reaffirm the commitments we've made directly to our customers*."

That's an untrue public representation.

This Student Privacy Pledge is actually a much stronger public commitment than the Google Apps for Education contractual commitments Google has made with school administrators. …When school administrators study the fine print in the context of this new Student Privacy Pledge, they will learn they have been duped into unwittingly signing a contract that does not actually fully protect their students from data collection for the ultimate purposes of monetization as Google represents. … Google's new Student Privacy Pledge requires Google to not collect and use student information for profit.

However, most people don't know that Google's Apps for Education's contracts only agree to not advertise to students on Google's "core" education products like Gmail, Docs, Drive, etc., but the contracts exclude many Google student-popular products like YouTube, Maps, Android, Play, Google+, Chrome, etc. that students clearly could need or demand in their Google Apps for Education experience.

This is a classic case of deceptive exceptions becoming the real rule. Thus, if students and school administrators are like most people, they would believe that the same privacy policy and protections would apply to all Google services that would be normally needed and used in schools, but they would be wrong."

8. Google-DoubleClick Combining Personal Data with Tracking Data

In December 2016 Consumer Watchdog filed a complaint with the FTC that Google violated the Google-Buzz consent decree in deceptively forcing a privacy policy change that allowed Google to combine its

users' personally-identifiable information with DoubleClick's vast browsing data, when Google has long represented to the public and to the FTC that it would not do so.

A Pro Publica investigation spotlighted the importance of Google reversing one of the most important parts of its privacy policy by removing this longstanding public promise: "*We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent*."

December 19, 2016, Consumer Watchdog and Privacy Rights Clearinghouse filed an FTC complaint:

> "*charging that Google violated the law and an earlier consent agreement when it forced a change in its privacy policy on users in a highly deceptive manner, without meaningful notice and consent. The Internet giant's action, taken on June 28, is an unfair and deceptive practice, violating Section 5 of the Federal Trade Commission Act and also violates the terms of the "Buzz Consent Agreement" Google signed with the agency, the two California-based consumer advocacy organizations' formal complaint said. ... Consumer Watchdog and Privacy Rights Clearing House asked the FTC to claw back all advertising revenue earned by Google since the date of the change, citing past privacy violations by the internet giant as evidence that lesser penalties would not be enough to make the company respect consumers' privacy rights.*"

The Consumer Watchdog complaint explains what Google's most serious violation of the FTC-Google-Buzz privacy decree may be.

> "*Less than four months after entering into the Buzz Consent Order, Google announced plans to fundamentally change its privacy policy and terms of service." The most significant change was that, while Google had previously kept users' data from each of its services separate, it was now fusing all of that data together. Influenced by the recent Consent Order, Google announced the change two months before it took effect in a blog post that stated clearly: The main change is for users with Google Accounts. Our new Privacy Policy makes clear that, if you're signed in, we may combine information that you've provided from one service with information from other services." The post also contained a video that was intended to provide a simple explanation of the shift. Google undertook extensive efforts to obtain public support for the policy change. The company posted advertisements everywhere from the New York City subways to the World Wide Web. The advertisements offered simplified explanations of things like "cookies," and declared "[w]e're changing our Privacy Policy. Not your privacy controls." Google emphasized that it remained committed to being "transparent about the information [Google] collects." Clearly, Google was proactively taking steps to head off any claim that it did not adequately inform users. Google was criticized because it did not give users the ability to opt out of the change. The FTC declined to take action. A number of global authorities, however, found that Google's new policies were in conflict with their countries' data protection laws."*

Pro Publica provided critical historical context for the Google change, which follows.

> "*Privacy advocates raised a ruckus in 1999 when DoubleClick purchased a data broker that assembled people's names, addresses and offline interests. The merger could have allowed DoubleClick to combine its web browsing information with people's names. After an investigation by the Federal Trade Commission, DoubleClick sold the broker at a loss.*

In response to the controversy, the nascent online advertising industry formed the Network Advertising Initiative in 2000 to establish ethical codes. The industry promised to provide consumers with notice when their data was being collected, and options to opt out.

Most online ad tracking remained essentially anonymous for some time after that. When Google bought DoubleClick in 2007, for instance, the company's privacy policy stated: "DoubleClick's ad-serving technology will be targeted based only on the non-personally-identifiable information."

In 2012, Google changed its privacy policy to allow it to share data about users between different Google services - such as Gmail and search. But it kept data from DoubleClick – whose tracking technology is enabled on half of the top 1 million websites – separate.

But the era of social networking has ushered in a new wave of identifiable tracking, in which services such as Facebook and Twitter have been able to track logged-in users when they shared an item from another website.

Two years ago, Facebook announced that it would track its users by name across the Internet when they visit websites containing Facebook buttons such as "Share" and "Like" – even when users don't click on the button. (Here's how you can opt out of the targeted ads generated by that tracking).

Offline data brokers also started to merge their mailing lists with online shoppers. "The marriage of online and offline is the ad targeting of the last 10 years on steroids," said Scott Howe, chief executive of broker firm Acxiom."

9. Google In-Store Tracking

July 31, 2017, per beSpacific:

"*EPIC filed a complaint with the FTC asking the Commission to investigate Google's tracking of in-store purchases. According to EPIC, Google collects billions of credit and debit card transactions and then links that personal data to the activities of Internet users. Google claims that it protects online privacy but refuses to reveal details of the algorithm that "deidentifies" consumers while tracking their purchases. EPIC's complaint asks the FTC to stop Google's tracking of in-store purchases and determine whether Google adequately protects consumer privacy.*

EPIC has filed several successful FTC complaints that led to FTC investigations, including complaints about changes to Facebook's privacy preferences and the launch of Google Buzz. EPIC has also focused on the adequacy of privacy techniques, with complaints against AskEraser (search histories that are not deleted) and Snapchat (images that do not "vanish"). EPIC's recent complaint against Google notes that the company is seeking to extend its dominance of online advertising to the physical world."

10. Google-YouTube Children Privacy

In April 2018, 20+ U.S. child advocacy, consumer and privacy groups filed a complaint with the FTC documenting how Google-YouTube publicly represented YouTube as serving people 13 or older, in practice it unfairly and deceptively marketed, advertised and provided content evidently targeted at younger children in violation of COPPA, the Children's Online Privacy Protection Act.

CNET reports: "*The crux of the complaint, the groups said, is that kids younger than 13 watch YouTube videos, even though the company's terms of service technically forbid them to do so. When anybody watches a YouTube video, the company collects certain types of personal information, such as location or what kind of device is being used, to help with ad targeting. The complaint says YouTube is violating COPPA because it doesn't get parental consent before collecting the data.*

"Google's violations are particularly egregious," the complaint reads. "Google had actual knowledge of both the large number of child-directed channels on YouTube and the large numbers of children using YouTube."

****