

July 21, 2022

To:

Kent Walker, President of Global Affairs, Google & Alphabet

Keith Enright, Chief Privacy Officer

Alicia Gray, Senior Manager, Android Privacy

With *Roe v. Wade* overturned, the massive stockpiles of deeply personal user data that Big Tech collects and retains could be weaponized against people providing, assisting, or seeking reproductive healthcare. Collectively more than 100,000 supporters of tech accountability have joined the call for [Google to stop unnecessarily collecting and retaining location data](#). With so many apps requiring location data to function (maps, ride-hailing apps, weather apps and more), even the most privacy-conscious users are likely sharing their location information with Google.

On July 1, Google [announced](#) it was changing its policies to delete data entries from [Location History](#) soon after users visit certain sensitive locations (counseling centers, domestic violence shelters, abortion clinics, etc.) In updating its policy, Google is acknowledging that the datasets it retains are potentially damaging and could be used against users - and that it has a responsibility towards protecting our privacy. Your company collects a virtually unimaginable amount of data - not only information about where we've been, but also what we've bought, what information we have sought, who we've talked to, what we've said, and more. Users have very little visibility into how that information is collected, collated, and used.

A recent [report](#) from the [Tech Transparency Project](#) demonstrates that Google's policy update has significant gaps, and we still have a *lot* of questions for Google about its data collection practices:

- 1. Will Google allow users to have a voice in deciding what constitutes "sensitive data" and is therefore worthy of redaction?** If "particularly personal" is the criterion, should Google not clear location information about residences or general visits to the doctors office as well? Since the *Dobbs* decision was announced there have also been increasing threats to LGBTQIA+ communities, as well as access to contraception, further increasing the need to protect a wide range of locations, especially LGBTQIA+ spaces or activist convenings as well as trans healthcare centers.
- 2. How will Google identify the locations (medical facilities like counseling centers, domestic violence shelters, abortion clinics, fertility centers, etc.) that trigger data deletion?** Even if we agree these "sensitive data" categories are appropriate, Google has to create some sort of geofencing that maps those categories to specific places - what are those boundaries? How wide of a margin gets omitted from the record? Are there time constraints? Does a location have to register with Google that it's a "sensitive" space at certain times?
- 3. Will you retain backups of the data you claim to be deleting, and if so, will you push back against potentially unlawful warrants or subpoenas, and provide notice to users when you receive them?** Once Google claims to delete a users' data, the user loses access to that data. However, it is unclear whether or not Google still keeps backup records once they claim to delete it, and if law enforcement can subpoena backup data. Google states it will "continue to push back on overly broad" demands from law enforcement, but it must do more to protect data privacy. How will Google decide what is considered "overly broad" and will it include people's location data, search data, and more that could be used to

prosecute an abortion case. Google has still not answered if they will cooperate with state or local government authorities requesting information on those seeking abortion care.

- 4. Will you provide more granularity on the type of data requests you receive from law enforcement authorities?** Details matter.
- 5. Are the systems that still get data locations even when Location History is off going to also respect the same dead zones?** Historically, [Google has misled users about its data collection policies](#) - even when users opt-out of location history, the tech giant *still* surveils users.
- 6. Will you give users an option to auto-delete location history data sooner than 3 months?** Acknowledging the data you hold is potentially damaging to users, there are many steps you can take to grant users greater agency over their data (e.g. allowing data to be deleted *immediately* after it is collected.)
- 7. Can you do more to mitigate the risk that a sudden gap in location data may be used as additional circumstantial evidence in court against those providing or seeking abortion care?**
- 8. What steps will you take regarding other user data?** The volume of data in Google's hands means that creative prosecutors will find other incriminating items in people's online records that no one ever imagined might be seized in this context. To help address that, Google should immediately take steps to confine the data it collects to only what is necessary to provide the service the user requests, limit data retention, and share the data, if at all, only with trusted and vetted third parties.

Google must serve as a responsible steward of the data it collects and enact real policy changes to protect users online.

The undersigned,

Accountable Tech
Access Now
Defending Rights & Dissent
Electronic Frontier Foundation (EFF)
Fight for the Future
GLAAD
Jewish Women International
Kairos
MediaJustice
Media Matters for America
Parents Together
Reproaction
#ShePersisted
Sum of Us
Tech(nically) Politics
UltraViolet