

Congress of the United States  
Washington, DC 20515

August 24, 2022

Loredana Crisan  
Head of Messenger  
Meta Platforms, Inc.  
1 Hacker Way  
Menlo Park, CA 94025

Will Cathcart  
Head of WhatsApp  
Meta Platforms, Inc.  
1 Hacker Way  
Menlo Park, CA 94025

Hans Vestberg  
Chief Executive Officer  
Verizon Communications Inc.  
1095 Avenue of the Americas  
New York, NY 10013

John Stankey  
Chief Executive Officer  
AT&T Inc.  
208 South Akard Street  
Dallas, Texas 75202

Tim Cook  
Chief Executive Officer  
Apple Inc.  
1 Infinite Loop  
Cupertino, CA 95014

Hiroshi Lockheimer  
SVP Platforms & Ecosystems  
Google LLC  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Dear Loredana Crisan, Will Cathcart, Hans Vestberg, John Stankey, Tim Cook, and Hiroshi Lockheimer,

We write to inquire about your company’s usage, storage, and sharing of phone call and messaging metadata, especially as it relates to protecting the privacy of individuals using your services to exercise their reproductive rights. As you know, with the recent U.S. Supreme Court decision to overturn *Roe v. Wade*,<sup>1</sup> more states are criminalizing abortion, and law enforcement entities have used digital evidence to punish people for seeking or providing abortion care.<sup>2</sup>

Phone call and messaging metadata—data collected *about* communications such as time, duration, and involved phone numbers—is characterized as less invasive and revealing because it does not disclose any content of the calls made or messages sent. This has been the prevailing argument for the “harmlessness” in bulk collection of this metadata. However, according to multiple investigations, this metadata can be used to build strong inferences about the services and projects people are pursuing, and the people with whom they interact with most closely.<sup>3</sup>

---

<sup>1</sup> *Abortion Policy in the Absence of Roe*, Guttmacher Institute, May 2022 at: <https://www.guttmacher.org/state-policy/explore/abortion-policy-absence-roe>

<sup>2</sup> Zakrzewski, Cat et al, *Texts, web searches about abortion have been used to prosecute women*, Washington Post, July 3, 2022 at: <https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/>

<sup>3</sup> Mayer, Mutchler, and Mitchell, *Evaluating the privacy properties of telephone metadata*, May 2016 at: <https://www.pnas.org/doi/full/10.1073/pnas.1508081113>

See also Zuckerman, Ethan, *Me and my metadata – thoughts on online surveillance*, July 2013 at: <https://ethanzuckerman.com/2013/07/03/me-and-my-metadata-thoughts-on-online-surveillance/>

Phone call and messaging metadata analysis could reveal a user's plans to obtain information about and seek abortion care by analyzing the timing, duration, and frequency of calls to abortion providers.<sup>4</sup> Even when this metadata is anonymized via hashing algorithms, it can still be de-anonymized with enough computing resources.<sup>5</sup>

In a post-*Roe* world, phone call and messaging metadata could be used as evidence to establish probable cause that someone has sought an abortion. Social graphs can be easily constructed to see who has helped these people seek abortion, leaving them vulnerable to prosecution as well.

Given the sensitivity of this data and its relevance to fundamental rights, we aim to understand the practices you have in place today and those you plan to adopt to protect this data. We request a response to the following by September 12, 2022:

1. Do you collect metadata about calls made or messages sent from an individual's device? If so, how is that metadata used, how long is it stored for, and who has access to it?
2. What kinds of controls do users have to view and delete their existing metadata? Can users opt out of future metadata storage? Can users restrict third party access to their metadata? How accessible are these controls?
3. What additional measures, if any, have you taken to secure the storage of this metadata?
4. Do you alert users when third party companies request phone call and messaging metadata access? Do you alert users when law enforcement requests phone call and messaging metadata access?
5. Has your company adopted any policies to restrict the disclosure of metadata that could be used to prosecute or otherwise harass those seeking reproductive healthcare to law enforcement or private actors? What steps do you take to enforce those policies?
6. Who is authorized or can be authorized to access the metadata you collect? Are there any limits on who can obtain access to metadata that can be used to prosecute people seeking reproductive healthcare?

Sincerely,



Lori Trahan  
Member of Congress



Diana DeGette  
Member of Congress



Barbara Lee  
Member of Congress

---

<sup>4</sup> Hern, Alex, *Phone call metadata does betray sensitive details about your life – study*, March 2014 at: <https://www.theguardian.com/technology/2014/mar/13/phone-call-metadata-does-betray-sensitive-details-about-your-life-study>

<sup>5</sup> Bradshaw, Kyle, *Google Phone & Messages address potential privacy concerns, reduce call & message metadata collection*, March 2022 at: <https://9to5google.com/2022/03/22/google-phone-messages-privacy-research-call-text-records/>



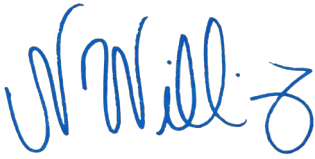
Eleanor Holmes Norton  
Member of Congress



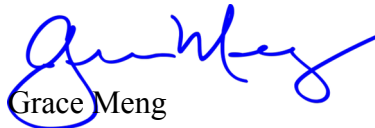
Rashida Tlaib  
Member of Congress



Bill Foster  
Member of Congress



Nikema Williams  
Member of Congress



Grace Meng  
Member of Congress



Nanette Diaz Barragán  
Member of Congress



Bonnie Watson Coleman  
Member of Congress



Cori Bush  
Member of Congress



Mark DeSaulnier  
Member of Congress



Sean Casten  
Member of Congress