10 March, 2021

To:
Michael Sievert, CEO, T-Mobile US
John T. Stankey, CEO, AT&T
Hans Vestberg, CEO, Verizon Communications:

Internet service providers (ISPs) are the gateway to the Internet. As companies with the ability to see and store much of their customers' browsing history, ISPs have a special responsibility to protect their customers.

We write to urge you to commit to limiting data collection and retention, and ensure transparency around how data is stored and used — including data sharing with business partners and affiliates for non-operational purposes.

DNS data can reveal a lot of sensitive information, and currently DNS providers aren't subject to strong legal or regulatory limits on what they can do with that data. That is why we are calling on you to act in good faith and to meet the demands of your customers, who are increasingly concerned with how their personal data is handled. This is especially concerning as so many Americans have turned to mobile connections in the midst of this global pandemic.

We believe that each and every customer paying for your internet service has the right to determine how their personal data will be used, on an opt-in basis. To that end, we are asking you to make three commitments with respect to consumer data:

1. Use DNS consumer data strictly for the purpose of providing DNS resolution services, unless the user has explicitly opted into secondary uses of the data;
2. Delete DNS resolution data after 24 hours, unless the user has explicitly opted in to use of the data strictly for legitimate security and forensic purposes; and
3. Refuse to sell, share, or license access to user data to other parties without first seeking the explicit and informed consent of your customers.

These three commitments serve to ensure that your customers' browsing habits are not used without their knowledge and that you have at least 24 hours of operational insight strictly for the purpose of operating your DNS service, unless consumers consent to a longer retention period for security and forensic purposes.

Transparency is an essential component of building customer trust in your brand, especially when it comes to the use of their personal data. Ultimately it is up to you to treat their data properly, which in the future might include publishing transparency reports or conducting audits by credible external parties, and committing to (1) making the audit report public in a timely manner, and (2) promptly addressing any deficiencies identified.

We are at a tipping point in consumer demand for stringent privacy protections and clear, honest communication from companies about how personal data is handled, modified, and stored. Given the growing awareness among consumers about privacy issues, and constant news about data breaches and inappropriate data use by companies in many industries, this marks an opportunity for service providers to explicitly use privacy as a key selling point – using it as a competitive differentiator.

Signed:

Article 19
Consumer Reports
Electronic Frontier Foundation
The Internet Society

Mozilla
New America's Open Technology Institute
Public Knowledge