

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

December 15, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan:

I write to request that the Federal Trade Commission (FTC) investigate Neustar Security Services' ("Neustar") sale of Americans' internet metadata to a Department of Defense (DOD)-funded research project at the Georgia Institute of Technology ("Georgia Tech"). Those researchers in turn repeatedly searched this data at the request of the Department of Justice (DOJ) and other government agencies.

For several years, Neustar knowingly sold sensitive internet metadata which it presumably obtained from unwitting consumers. Some of these consumers may have been promised that their data would not be sold to third parties. Neustar did not take sufficient steps to warn consumers that it no longer intended to honor these promises, and as such, appears to have engaged in business practices substantially similar to those that the FTC has previously argued violated the FTC Act.

Neustar collects information about which websites its customers visit as part of its "recursive Domain Name System (DNS)" service, which looks up the domain name that a user is trying to access, such as ftc.gov, and connects it to a specific IP address. Companies that provide recursive DNS services receive extremely sensitive information from their users, which many Americans would want to remain private from third parties, including government agencies acting without a court order. For example, knowing that a user visited the website of the National Suicide Prevention Hotline (suicidepreventionlifeline.org), the National Domestic Violence Lifeline (thehotline.org) or Power to Decide's Abortion Finder service (www.abortionfinder.org) can all reveal deeply personal and private information about a person.

As the Wall Street Journal described earlier this year, starting in the fall of 2016, Neustar began selling DNS data to a DoD-funded research team at Georgia Tech. Emails obtained by the press and activists from Georgia Tech under Georgia's Open Records Act document the sale of data under a five year, nearly \$2 million contract. Neustar has refused to answer questions about its sale of this data, but in a September 8, 2022 briefing with my staff, said that it does not currently sell DNS data. After my staff attempted to confirm in writing the statements Neustar representatives made during that briefing, Neustar's counsel responded on September 16, 2022 by email that the company "does not sell DNS data to governments, including the United States government."

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

The Georgia Tech emails confirm that this DNS data was not solely used for academic research. The emails include several communications between the researchers who purchased the data and both the FBI and DOJ, indicating that government officials asked the researchers to run specific queries and that the researchers wrote affidavits and reports for the government describing their findings. The publicly released emails referencing these DOJ requests for assistance do not indicate whether they were accompanied by a warrant. My office has repeatedly requested information about the DOJ's requests for DNS data from Georgia Tech, but the DOJ has refused to provide my staff with any information. However, federal government agencies have repeatedly argued that the Fourth Amendment does not apply to data the government purchases.

In addition to Neustar's well-documented sale of data to Georgia Tech, recent court testimony suggests that former Neustar executive Rodney Joffe, who led the company's efforts to sell data to Georgia Tech, was also involved in the sale of DNS data directly to the U.S. government. During the recent criminal prosecution of another individual, federal prosecutors and the defense agreed to a stipulated statement that was entered into the court record, which stated:

Rodney Joffe and certain companies with which he was affiliated, including officers and employees of those companies, have provided assistance to and received payment from multiple agencies of the United States government. This has included assistance to the United States intelligence community and law enforcement agencies on cyber security matters. Certain of those companies have maintained contracts with the United States government resulting in payment by the United States of tens of millions of dollars for the provision of, among other things, Domain Name System ('DNS') data. These contracts included classified contracts that required company personnel to maintain security clearances.

Neustar's sale of DNS data may have been a deceptive business practice

Representatives from Neustar told my staff during a September 8, 2022 briefing that the only user-level DNS data the company holds comes from users of recursive DNS services provided by the company. As such, the data that Neustar sold to Georgia Tech likely included data generated by users of the free recursive DNS service that Neustar had long offered to the public. While Neustar had, since at least 2013, included language in its privacy policy indicating that it might share data with third parties, the FTC has made it clear that disclosures of practices that materially impact consumer privacy must be prominently disclosed to consumers and that disclosures in privacy policies are insufficient.

As the FTC noted in its complaint against Sears Holdings in 2009, companies have an obligation to disclose "facts [that] would be material to consumers in deciding to install the [company's] software." In the same case, the FTC held that failure to disclose these facts can be a deceptive practice. Moreover, as the FTC wrote in its 2013 staff report on .com disclosures, "it is highly unlikely that consumers will read disclosures buried in 'terms of use' and similar lengthy agreements. Even if such agreements may be sufficient for contractual or other purposes, disclosures that are necessary to prevent deception or unfairness should not be relegated to them."

The data that Neustar sold to Georgia Tech may have also included data collected from consumers who were explicitly promised that their data would not be sold to third parties. Between 2018 and 2020, Neustar acquired a competing recursive DNS service, which had previously been operated by Verisign. That service had been advertised to the public by Verisign with unqualified promises that “your public DNS data will not be sold to third parties.” When the product changed hands, users of Verisign’s service were seamlessly transitioned to DNS servers that Neustar controlled. This meant that Neustar now received information about the websites accessed by these former Verisign-users, even though neither Verisign nor Neustar provided those users with meaningful, effective notice that the change of ownership had taken place, or that Neustar did not intend to honor the privacy promises that Verisign had previously made to those users.

It is unclear if the data Neustar sold to Georgia Tech included data from users who had been promised by Verisign that their data would not be sold. This is because both Neustar and Verisign have refused to answer questions from my office necessary to determine this important detail. My staff spoke with Neustar on September 8, 2022 and Verisign on September 7, 2022. Neustar would only say that it is not currently selling DNS data and refused to discuss its past practices. These two companies refused to discuss the source of the data Neustar sold to Georgia Tech, when Neustar stopped selling this data, whether it only included data from users of Neustar’s legacy DNS service, whether it included data from users who originally signed up for Verisign’s DNS service, and whether Verisign contractually required Neustar to continue to honor the privacy commitments it had made to its users.

However, both companies cited their issuance of a press release and posts on their respective websites as sufficient notice to consumers that the privacy terms had changed. This is simply unacceptable. Consumers using Verisign’s free DNS service had no reason to regularly check the company’s website, as long as their DNS service kept working. While it is true that Verisign did not collect email addresses or phone numbers of users of its service, and therefore did not know who they were or how to contact them to notify them of the change in ownership, that does not mean that Verisign and Neustar could force a new, far more permissive privacy policy on unknowing users. Verisign and Neustar, collectively, had an obligation to ensure the privacy commitments made by Verisign were honored, to find a way to notify users of the change in policy, or to shut down the service.

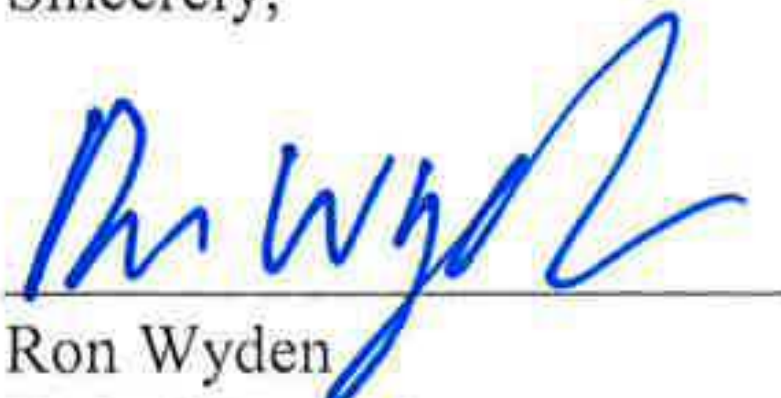
Indeed, the FTC has made it clear that privacy promises to consumers must be honored, even when a product changes hands, and that a company that buys another company must obtain opt-in consent from consumers before abandoning privacy commitments made by the prior owner. For example, the FTC sued Toysmart.com in 2000 after the company, which had promised consumers in its privacy policy that their data would “never be shared with a third party,” went bankrupt and began soliciting bids for its customer list. While the FTC ultimately allowed Toysmart’s customer data to be sold to another company, it required that the buyer honor the promises that Toysmart made in its privacy policy and to seek affirmative consent from consumers before making any changes to the privacy policy. This case is not an isolated exception. After RadioShack’s bankruptcy in 2015, the FTC wrote to the court-appointed ombudsman and urged her to adopt a similar set of restrictions as the FTC had obtained in Toysmart.

Regardless of whether the data Neustar sold included data from users who originally signed up when the service was offered by Verisign, it is clear that Neustar sold DNS data for millions of dollars to researchers at Georgia Tech. If this data was obtained from Neustar customers, then it appears that Neustar failed to sufficiently warn consumers about its sale of their browsing data, and may have engaged in deception through a material omission. And in the worst case, Neustar may have deceived consumers who had been explicitly promised by Verisign that their data would not be sold. These potentially deceptive practices resulted in the subsequent sharing of Americans' data with U.S. government agencies, apparently without a warrant.

Given the refusal by Neustar and Verisign to clear up the facts, I urge the FTC to investigate this matter, and where appropriate, hold these companies accountable.

Thank you for your attention to this important matter.

Sincerely,



Ron Wyden
United States Senator