HOUSE OF REPRESENTATIVES

DAVID SCHWEIKERT, ARIZONA, CHAIRMAN
JODEY C. ARRINGTON, TEXAS
RON ESTES, KANSAS
LLOYD K. SMUCKER, PENNSYLVANIA
NICOLE MALLIOTAKIS, NEW YORK
VICTORIA SPARTZ, INDIANA

DONALD S. BEYER JR., VIRGINIA
GWEN MOORE, WISCONSIN
SEAN CASTEN, ILLINOIS
DAVE MIN, CALIFORNIA

RON DONADO, EXECUTIVE DIRECTOR

Congress of the United States

JOINT ECONOMIC COMMITTEE
(CREATED PURSUANT TO SEC. 5(a) OF PUBLIC LAW 304, 79TH CONGRESS)

Washington, DC 20510–6602

SENATE

ERIC SCHMITT, MISSOURI, VICE CHAIRMAN
TOM COTTON, ARKANSAS
TED BUDD, NORTH CAROLINA
DAVID McCORMICK, PENNSYLVANIA
MARSHA BLACKBURN, TENNESSEE
ASHLEY MOODY, FLORIDA

MARGARET WOOD HASSAN, NEW HAMPSHIRE,
RANKING MEMBER
AMY KLOBUCHAR, MINNESOTA
MARTIN HEINRICH, NEW MEXICO
MARK KELLY, ARIZONA

LAURA EPSTEIN, DEMOCRATIC STAFF DIRECTOR

February 3, 2026

Mr. Fateen Anam Rafid
Founder and CEO
bondu
1525 Van Ness Avenue
San Francisco, CA 94109

Dear Mr. Anam Rafid:

I write today seeking information about an extensive security vulnerability, recently reported by *WIRED*, that resulted in the public exposure of bondu's users' personally identifying information as well as more than 50,000 transcripts of conversations that users had with bondu's interactive AI toy. This AI toy is marketed to children between the ages of three and nine years old, making the exposure of their information particularly devastating.[1] The gravity of this exposure raises serious concerns regarding the business model your company has adopted and your efforts to anticipate and prevent significant threats to the safety and privacy of children.

According to *WIRED*, two security researchers – using only a Gmail account and no specialized tools – navigated bondu's public websites and accessed a web-based company portal that contained "transcripts of virtually every conversation [b]ondu's child users have ever had with the toy" in a matter of minutes.[2] Despite having no special accounts or affiliations with bondu, these researchers acquired "full access" to a range of sensitive information, including children's names and birthdates, family member names, and the likes and dislikes of child users.[3] They concluded that this level of access "was all available to *anyone with a Google account*."[4]

[1] *An AI Toy Exposed 50,000 Logs of its Chats with Kids to Anyone with a Gmail Account*, WIRED (Jan. 29, 2026) (www.wired.com/story/an-ai-toy-exposed-50000-logs-of-its-chats-with-kids-to-anyone-with-a-gmail-account/); bondu, Meet bondu (bondu.com/) (accessed Jan. 30, 2026).

[2] *Id*.

[3] Justin Thacker, *Hacking an AI Children's Toy: Remote Access to Every Conversation*, Joseph Thacker Blog (Jan. 29, 2026) (josephthacker.com/hacking/2026/01/29/bondu-smart-toy-vulnerability.html).

[4] *Id*.

Although *WIRED* reports that bondu quickly acted to remedy these security issues, the potential risks from these vulnerabilities are profound.[5] Identity thieves, for example, target children in order to open new accounts, apply for government benefits, or take out loans – activities that a child victim may not discover until reaching adulthood.[6] More disturbingly, information in private chat transcripts could facilitate crimes against children; one researcher warned: “We're talking about information that lets someone lure a child into a really dangerous situation.”[7]

The reporting also calls into question the safety and security claims that bondu has made publicly. The company claims, for example, that it uses “industry-standard safeguards such as encryption and secure authentication to protect your account.”[8] In addition, the bondu website states that “[a]ccess to any personal data is strictly limited to authorized core team members who need it to support your experience.”[9] One of the researchers who accessed the bondu data noted, however, that the “whole team [at bondu] shares customer support work, so they all had access.”[10]

Given the vulnerabilities at bondu that left children’s data unprotected – and the serious consequences that can occur if criminals obtain this data – I seek responses to the questions below.

“Security vulnerability/vulnerabilities” mentioned here reference vulnerabilities that security researchers Joseph Thacker and Joel Margolis identified. Unless otherwise specified, “user data” refers to the information that these researchers could access as described in a January 29, 2026, blog post by Mr. Thacker, including but not limited to personally identifying information, chat histories, and device information.

[5] *An AI Toy Exposed 50,000 Logs of its Chats with Kids to Anyone with a Gmail Account*, WIRED (Jan. 29, 2026) (www.wired.com/story/an-ai-toy-exposed-50000-logs-of-its-chats-with-kids-to-anyone-with-a-gmail-account/).

[6] Federal Trade Commission, *How to Protect Your Child From Identity Theft* (Oct. 2024) (consumer.ftc.gov/articles/how-protect-your-child-identity-theft#what_is).

[7] *An AI Toy Exposed 50,000 Logs of its Chats with Kids to Anyone with a Gmail Account*, WIRED (Jan. 29, 2026) (www.wired.com/story/an-ai-toy-exposed-50000-logs-of-its-chats-with-kids-to-anyone-with-a-gmail-account/).

[8] bondu, FAQ (bondu.com/pages/faq) (accessed Jan. 30, 2026).

[9] *Id*.

[10] Justin Thacker, *Hacking an AI Children’s Toy: Remote Access to Every Conversation*, Joseph Thacker Blog (Jan. 29, 2026) (josephthacker.com/hacking/2026/01/29/bondu-smart-toy-vulnerability.html).

1. What steps has bondu taken to remedy the user data vulnerability uncovered on January 10, 2026?

    a. Has bondu alerted customers about the risks to their data from this security vulnerability? Relatedly, how many child users did this vulnerability impact?

    b. What authentication measures has bondu added to its portal? What additional preventative measures or protections has bondu implemented in response to identified vulnerabilities?

    c. Please describe findings from any security reviews bondu has conducted in response to identified vulnerabilities.

    d. Does bondu conduct ongoing monitoring of its portal to detect unauthorized access? If bondu has not detected unauthorized access to the portal, please provide the basis for this determination.

2. How long does bondu retain user chat transcripts and for what reasons? Does bondu store user data in other places outside of its portal, including with third parties?

3. Please describe the privacy and data security testing that bondu conducted prior to the release of current bondu products.

4. The company states on its website that it uses “industry-standard safeguards such as encryption and secure authentication to protect your account.” What, if any, user information does bondu encrypt?

    a. Please describe the “secure authentication” measures that bondu deploys to protect accounts.

5. How many bondu employees have access to users’ personal data through the company’s portal or through other means? Please also provide the total number of bondu employees.

    a. What data, specifically, can authorized employees access, and how do they use this data?

    b. Following the discovery of the security vulnerability described above, does bondu intend to restrict employee access to this data?

6. Did bondu program its portal using AI tools, and if so, what efforts did the company undertake to detect potential security flaws that could arise in connection with this approach?

7. What type of monitoring does bondu undertake of the chat logs produced by its product?

a. Does bondu monitor for signs of abuse or violence committed against children?
i. If so, what processes does bondu have in place to report those events to law enforcement?
ii. How many reports to law enforcement has bondu made?

b. Does bondu review data before deletion by a parent/guardian to ensure that the data deleted is not evidence of a crime?
i. Can bondu recover deleted data?

8. What, if any, rights to their data do minor users of bondu have?

a. Is there a process in place for minor users of bondu to request that their data be deleted?

b. Is there a process in place for adults who previously were minor users of bondu to request that their data be deleted?

9. How does bondu confirm that the purchaser of its product and/or the user of the connected app are adults?

a. How does bondu confirm that those adults are the parents or legal guardians of the child who is using the product?

b. Does bondu provide any privacy protections for children who create data on a bondu product not owned by them or their family?

10. Can bondu remotely access and/or activate its products? If so, which employees at bondu have this ability and what limits are put on that ability?

Please provide your responses as soon as possible but in no event later than February 23, 2026. [redacted]

Sincerely,

Maggie Hassan

Margaret Wood Hassan
Ranking Member

cc: David Schweikert
Chairman

Eric S. Schmitt
Vice Chairman