**Before the**
**Federal Trade Commission**
**Washington, DC 20580**
**via E-mail: opa@ftc.gov**

| | |
|---|---|
| **In the Matter of** | **]** |
| | **]** |
| **uKnowKids** | **]** |
| **(uKnow.com)** | **]** |

**March 26, 2016**

**REQUEST FOR INVESTIGATION AND**
**COMPLAINT FOR INJUNCTIVE RELIEF**

## OVERVIEW

**uKnow.com** describes their **uKnowKids** service as a "Parental Intelligence System" that "helps protect kids from predators, bullies and sexting" and enables parents to "have their child's back" without constantly looking over his or her shoulder[1]. The firm claims that it "gathers and analyzes social and mobile data from 21 different data sources in order to help make your life as a digital parent easier and simpler,[2]" and "helps moms and dads keep their kids safe on their iPhones, iPads, iPods, and Android mobile phones by giving parents an inside look at their social network activities, text messages, iMessages, phone calls, digital contacts, installed mobile apps, and photos they share with their friends and strangers.[3]"

Stripped of its advertising hype, uKnowKids is a child tracking and monitoring service where children may not know they are being tracked or monitored by their parents. Not only may they be monitored and/or tracked on the Internet and on devices without their knowledge or consent, but it appears to be the case that other children who interact with them may also have their public and private communications collected, shared, and/or stored without their knowledge or their parents' consent, which would seem to violate COPPA (16 CFR Part 312).

This complaint also raises questions about whether uKnow.com engaged in unreasonable security practices that placed children's personal and sensitive information at risk of substantial injury or harm from hackers or bad actors who could have easily acquired and dumped personal and sensitive communications.

## PARTIES

**"Dissent"** is the pseudonym of a privacy advocate who publishes PogoWasRight.org and DataBreaches.net, two non-commercial blogs oriented to increasing consumer awareness of issues affecting their privacy. Her blogs accept no advertising or sponsorship and she is not employed in the field of security or privacy. This complaint is submitted in her personal capacity as a privacy advocate.

---

[1] https://www.uknowkids.com/our-story/
[2] https://www.uknowkids.com/features/
[3] http://www.uknow.com/

On their web site, **uKnow.com, Inc.** lists their address as 1400 Key Boulevard, Arlington, Virginia, 22209. uKnow.com's course of business has been, and is in or affects commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

STATEMENT OF FACTS[4]

1. When parents sign up for the uKnowKids service, they create a profile, to which they "add account information for online services, mobile telephone and other mobile device accounts belonging to you (the "Linked Accounts"). Of note, parents are required to warrant and represent that they are the legal owner of the accounts. From uKnow.com's Terms of Service[5]:

   > **You are the Legal Owner of the Linked Accounts**
   >
   > You warrant and represent to us that you own the Linked Accounts. Specifically, although Linked Accounts may be established in the names and using credentials for your minor children, you warrant and represent to us that you are the legal owner of all Linked Accounts and you have the legal authority to connect the Linked Accounts to the Services. You agree that it is your sole responsibility to ensure that all accounts used by your children that you wish to monitor are set up as Linked Accounts. Additionally, you agree that various laws may apply to the monitoring of Linked Accounts and that it is your sole responsibility to ensure compliance with any such laws and that uKnow.com expressly disclaims any duty or obligation to do so.

   It would appear from that last sentence that uKnow.com is attempting to absolve itself of all responsibility and liability should they be collecting or storing information on children or others in violation of any state laws or COPPA. But punting responsibility to parents who are unlikely to know state and federal laws protecting children's privacy seems inconsistent with the legislative intent and language of COPPA that makes businesses responsible for obtaining consent for information they collect, share, and store.

2. A key feature of the uKnowKids service is a parenting dashboard that they describe as "The All-inclusive Tool for Monitoring Your Child's Digital and Mobile Activities." The dashboard pulls in all activity from all of the "Linked Accounts," as illustrated in their demo screencaps,[6][7] below:

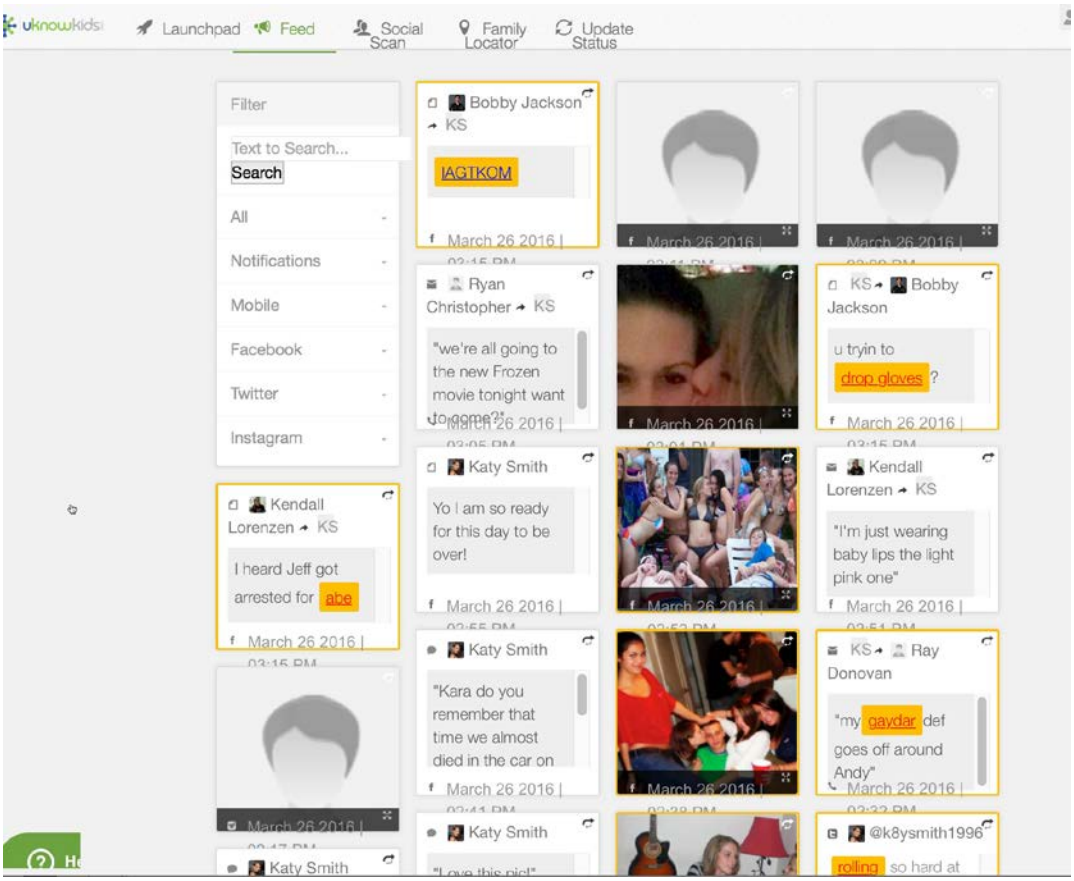
[4] The complainant is aware that uKnow.com claims it self-referred a recent data security incident to the FTC to seek advice. While that incident is part of this complaint, it is not the sole issue raised in this complaint.

[5] https://www.uknowkids.com/terms-service/

[6] https://app.uknowkids.com/summary.php

[7] https://app.uknowkids.com/timeline.php


*Screencap from Demo*




*Screencap from Demo Feed*

3. To the extent that the dashboard collates and merely links to urls that are publicly available, I see no issue. But to the extent that the dashboard is collecting and displaying private communications from non-targeted children (such as non-public facebook pages, photos sent privately, iMessages, Direct Messages on Twitter, etc.) and to the extent uKnowKids may share, copy, store, and/or backup such images and records in a cloud database, I think there may be issues under COPPA. The demo screencaps indicate that non-targeted children's private messages and communications are being displayed to the parent-customers without the consent of those children's parents.

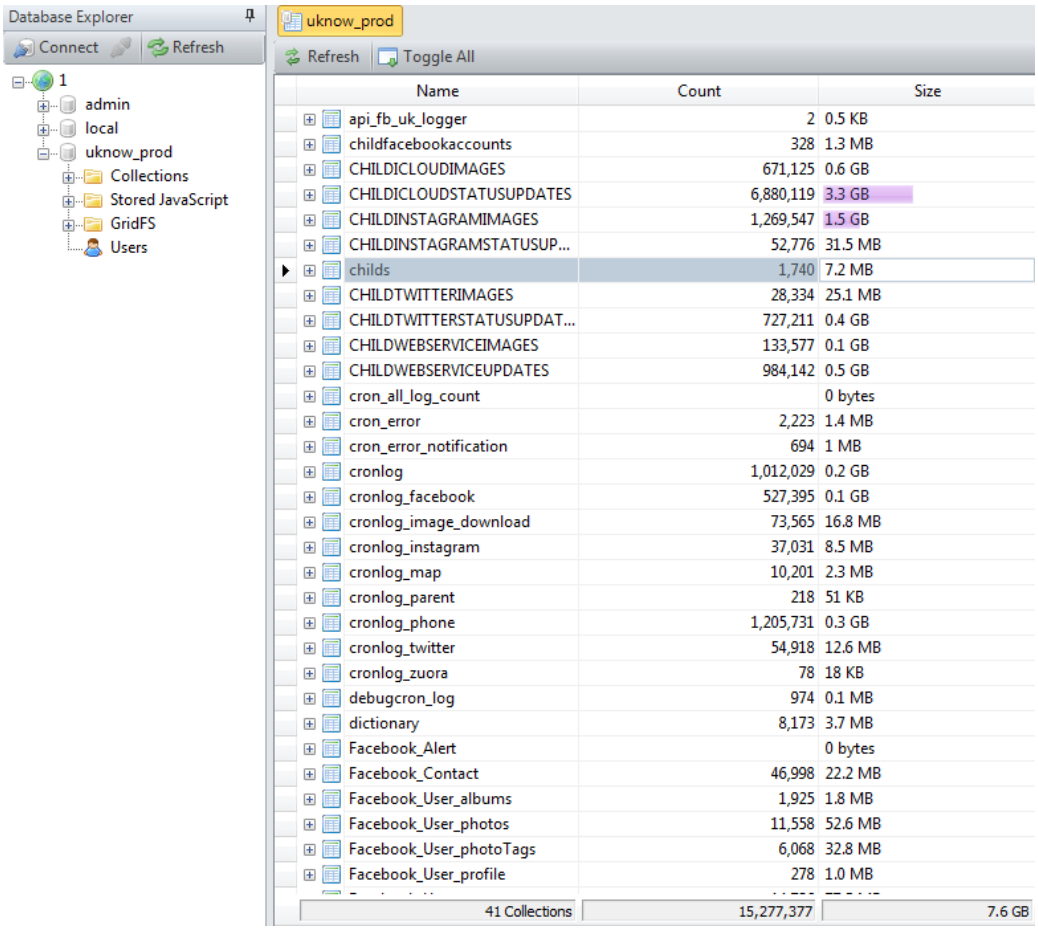
DATA SECURITY INCIDENT EXPOSES CHILDRENS' COMMUNICATIONS

4. On February 23, researcher Chris Vickery reported that due to a misconfigured MongoDB database installation, uKnowKids had exposed personal information of 1,740 kids:

> uKnowKids.com gave public access to over 6.8 million private text messages, nearly 2 million images (many depicting children), and more than 1,700 detailed child profiles. This includes first and last names, email addresses, dates of birth, gps coordinates, social media access credentials, and more[8].

5. The following screen cap taken from the exposed production database, was sent to me by Vickery:

[8] https://mackeeper.com/blog/post/192-uknowkidscom-database-error-exposed-sensitive-information-on-1700-kids

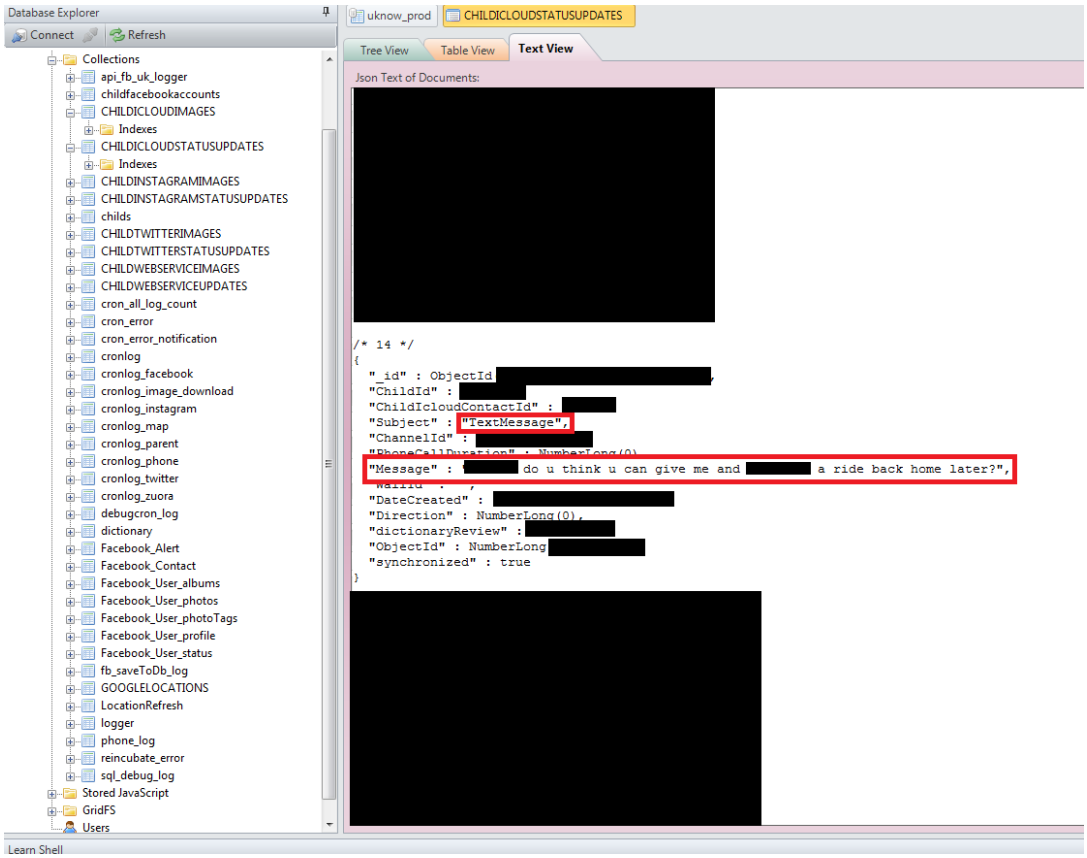



Note that in the screencap, one of the files refers to "childicloudimages."

6. Steve Ragan of CSOonline also reported on the incident and provided additional screencaps obtained from Vickery[9].

7. As Vickery reported, absolutely no authentication or login was required to access and download all those files, which – based on the filenames in the database and Vickery's observations - may have included iCloud images and communications from children whose parents were not signed up for the service but who had interacted with the tracked and monitored children. Also of note, the redacted screencaps in Ragan's report indicate that the files were in plain-text and not encrypted, as illustrated in a redacted screencap from the icloudstatusupdates file, below:

[9] http://www.csoonline.com/article/3036556/security/uknowkids-com-responds-to-data-breach-says-proprietary-ip-also-exposed.html




8. According to Vickery, metadata on Shodan suggested that the database had possibly been exposed for 48 days. uKnowKids would later provide more details[10] and report the exact timeframe[11]. Steve Woda of uKnowKids also claimed that their forensic examination revealed that it appeared that only Vickery's IP address had accessed any of the data while it was exposed.

9. This complainant does not dispute any of Woda's statements as to the time frame or downloading of data, but notes that the problem of misconfigured MongoDB database installations had been receiving attention for more than one year, (cf, coverage of one study finding 40,000 misconfigured databases[12] ). Other coverage in the year prior to uKnowKids' incident highlighted the problem in reporting on similar incidents involving HelloKitty, OKHello, MacKeeper, Alliance Health, Systema Software, and a database with 191 million

[10] http://www.databreaches.net/uknowkids-database-exposed-personal-and-location-info-of-1740-kids/ As this blogger commented in this and subsequent articles on this incident, uKnowKids' incident response, while commendable for its speed, was wildly inappropriate in suggesting the researcher was a criminal hacker. Any Google search on Vickery would have immediately revealed he's a white hat who responsibly discloses and has cooperated with law enforcement and the responsible entities. "Shooting the messenger" instead of thanking the messenger only discourages others from coming forward to notify entities when breaches or vulnerabilities are discovered. While the FTC has helpfully taken note in its guidance of the need to provide researchers and others with convenient ways to contact entities to report problems, the FTC may wish to consider issuing some additional guidance on how to respond to such notifications in ways that promote responsible disclosure and not punish it by defamatory public statements.

[11] http://resources.uknowkids.com/blog/uknowkids-data-breach-update

[12] http://news.softpedia.com/news/About-40-000-MongoDB-Databases-Found-Open-Online-472747.shtml

voters' records, to name just some of the stories that should have alerted uKnowKids to check their configuration and security of their database.

10. In their update on their breach report, uKnowKids provided a breakdown of the exposed data types:

| | Summary Data | Unique Child Profiles |
|---|---|---|
| Parent Accounts | 1,186 | 1,352 |
| Parent Email Addresses | 243 | - |
| Child Email Addresses | - | - |
| Credit Card Payment Information | - | - |
| uKnowKids Passwords | - | - |
| Data Channel Passwords | - | - |
| Mobile Image URLs | 1,068,250 | 1,086 |
| Social Network Image URLs | 905,791 | 670 |
| Social Network Posts | 413,629 | 856 |
| Mobile Messages | 6,346,161 | 1,189 |
| Social Network Tags | 6,026 | 233 |
| Social Network Contacts | 47,766 | 273 |

The data analysis does not indicate how many children who are not targeted children may have had their information exposed. *Were* their data exposed, and if so, how many children were affected? When uKnowKids issued a statement that they had notified the FTC and its customers, their statement made no mention of non-subscribers' children whose data may have been exposed, and it is not clear based on their statements whether any such children had data involved in the incident.

11. On February 25, after reporting[13] on the incident and uKnowKids' response – which didn't address any non-targeted children whose data might have been exposed, I contacted uKnowKids to inquire:

> One question that does not seem to have been addressed by Mr. Woda is that in the process of collecting and storing information on to-be-tracked/monitored children, did uKnowKids collect and store information about those children's friends and contacts without those children's knowledge and without their parents' consent?
>
> How many, if any, of the tracked children's friends and contacts had their pictures and/or messages and/or details exposed through uKnowKids' failure to secure the MongoDB installation?

They never answered those direct questions, despite repeated inquiries on my part. Instead, they repeatedly pointed me to their TOS and site and marked my inquiries "solved," without ever directly answering the questions about non-targeted children.

So… how many children, if any, has uKnowKids collected personal information from and about without their parents' consent? And if uKnowKids does collect information, can it share it with other parents and/or store it without their parents' consent? If so, how many of them had their

[13] http://www.databreaches.net/uknowkids-database-exposed-personal-and-location-info-of-1740-kids/

personal information exposed by uKnowKids' infosecurity failure[14]?

QUESTIONS FOR THE FTC

12. Under COPPA, can a commercial service *collect and share* non-public personal information on minor children whose parents have NOT consented to the collection and sharing of their children's information? If COPPA aims to protect minor children, then uKnowKids should not collect and share information on other children incidental to providing information to subscribed parents about their own children's activities. But are they?

13. Under COPPA, can uKnowKids or any other commercial service *store* non-public personal information on minor children whose parents have NOT consented to the collection or storage of their children's information? Are uKnowKids storing such information in a database as Vickery's observations suggested?

14. Is uKnow.com's Terms of Services making their customers solely responsible for compliance with all laws regarding monitoring and tracking of children enforceable or is it an unacceptable attempt to evade accountability and liability?

15. Under Section 5 of the FTC Act, do the collection, sharing, and/or storage of non-public communications of minor children without their parents' consent constitute an unfair practice? For purposes of this question, the injury or harm is invasion of privacy.

16. Is it an unfair practice under Section 5 of the FTC Act if uKnowKids is monitoring or tracking children or adolescents without the children's knowledge or consent if the children actually own the devices that are being tracked? Is a parent's "warrant and representation" of ownership of accounts sufficient due diligence to protect the rights and privacy of children?

17. In the event of a data security breach, does uKnowKids.com have a duty to notify children or adolescents whose photos, iMessages or other personal info have been exposed, or is it sufficient to just notify their parents? Parents who never told their children they were being tracked will likely not tell them that their personal and sensitive info has been exposed (or may even be on a pedophilia site somewhere in another scenario).

18. In the event of a data security breach, does uKnowKids.com have an obligation to notify those whose data may have been collected and/or stored without their knowledge or consent by virtue of them interacting with a tracked/monitored child?

REQUEST FOR RELIEF

19. If FTC's investigation reveals that uKnowKids has been collecting and sharing non-public personal information of minors whose parents have not consented to the data collection and sharing, they should be required to cease and desist, and to purge all records previously collected. They should also have to provide individual notification to those whose data have been illegally collected, stored, and/or shared, and if that's not feasible, issue a public statement in prominent media outlets explaining what they had done.

[14] Although there is no evidence that the data were actually acquired by anyone other than the researcher, the complainant agrees with FTC's argument in FTC v. LabMD that Section 5 does not require the FTC to wait for harm to be done to protect the public as long as the significant harm is likely.

20. If FTC's investigation reveals that uKnowKids has been *storing* non-public communications and information on minor children whose parents have not consented to or subscribed to their service, uKnowKids should be required to cease and desist such data storage, securely purge all stored data, and notify those whose data they improperly stored. In the event that they do not have adequate contact information to provide individual notifications, they should be required to issue a notice in prominent media outlets.

21. Because uKnowKids' failure to secure their database - despite ample warnings in media reports over the preceding year - resulted in the personal information of children being left vulnerable to pedophiles, criminals, and others who might easily find the open database via a search using the Shodan search engine, uKnowKids should be required to have monthly third-party tests of the security of all databases containing information on minor children and/or should be required to deploy greater security for data at rest.

22. Any other relief the Commission deems just and proper under COPPA and/or Section 5.

I reserve the right to supplement this petition as other information relevant to this issue becomes available.

Should the FTC require any additional information from me, you may reach me via e-mail to admin@pogowasright.org or mailto:admin@databreaches.net.

Respectfully submitted,

"Dissent"