The Internet Already Knows I’m Pregnant

Kashmir Hill - kashmir.hill@gizmodo-media.com - @kashhill
Cooper Quintin - cooperq@eff.org - @cooperq
Intro

Kashmir
• Journalist
• Privacy Expert
• New Mother

Cooper
• Hacker
• Privacy Activist
• Cares about privacy issues for people with wombs
Anti-Choice Groups Use Smartphone Surveillance to Target ‘Abortion-Minded Women’ During Clinic Visits

May 25, 2016, 6:52pm  Sharona Coutts

Women who have visited almost any abortion clinic in the United States have seen anti-choice protesters outside, wielding placards and chanting abuse. A Boston advertiser’s technology, when deployed by anti-choice groups, allows those groups to send propaganda directly to a woman’s phone while she is in a clinic waiting room.
How to hide a baby bump
Retailers want to know who’s preggers

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start...
How not to hide it
What apps we tested

pTracker
Glow
nurture
cue
eve
what to expect
pregnancy+
webmd baby
pinkpad
flo

my calendar (Book)
mycalendar (Face)
fertility friend
get baby
babypod
BabyBump
Ovia
The Bump
Maya
The logos
Why people use these apps

Glow supports your personal health tracking from period to parenting. Choose your experience here!

Avoiding pregnancy
Gain insights on your body and fertility patterns to avoid pregnancy.

Trying to conceive
Receive accurate predictions on your fertility to boost your chances of pregnancy.

Fertility treatments
Manage the details of your medications, appointments, and results.

Birth Stories
horrific story!
Everything in my pregnancy was so easy! No morning sickness,...

362 26  Last reply 2 days ago

Baby Bump Selfies
37 weeks exactly 😛💙👶
Can't wait to meet my love 💙💙💙

51 2  Last reply 12 hours ago

Period Talk
Why is it greenish black

TMI
What these apps ask about

Did you take your prenatal vitamin?
Did you do kegels? (set of ten 3x a day)
Vaginal discharge?
Update your weight
Did you exercise?
Did you drink water?
Your sleep duration
Who figured out I was pregnant

Twitter
These people. (My inbox at 6 months)
Fun with Fine Print

What To Expect privacy policy
4000 words = 8 pages long
The What to Expect ‘Select Partners’ List
How This Can Go Wrong

Not everyone who gets pregnant stays pregnant.

The Internet Thinks I’m Still Pregnant

Modern Love
By AMY FITTMAN | SEPT 2, 2019
Fun with Fine Print

The Bump privacy policy
4700 words = 10 pages
If you use this feature to call a third party, we will record the phone call and any message you leave for the third party, as well as call information such as the number dialed, the date and time of the call and its duration, and your location as determined by your area code or as otherwise permitted.
WTF

~Contacted The Bump~

Their response: “[W]e do not record phone calls. The language is legacy language from prior contemplated features for The Knot that we do not use in either The Knot or The Bump apps. I've sent a note to my legal team to update this language in our privacy policy.”
Fun with Fine Print

Ovia Terms of Use

6,100 words = 14 pages
Downloader, beware

“Please do not ask Ovia Health for--or rely on--anything we communicate as medical advice. Although our apps, website, images, content, and communications may reference medical topics, we make no warranty whatsoever that any of the articles are accurate, up to date, or error free.”
That sounds a lot like medical advice.
RESULTS: “Data from 20 websites and 33 apps were collected. Of all the websites and apps used, one website and three apps predicted the precise fertile window.”
## Their Findings

Table 2. Fertility Windows and Ovulation Dates Predicted by Android Applications Compared With the Average U.S. Fertility Period (Gold Standard)*

<table>
<thead>
<tr>
<th>Application No.</th>
<th>Predicted Fertile Window (January)</th>
<th>Predicted Date of Ovulation</th>
<th>No. of Days Outside the Fertile Window</th>
<th>No. of Fertile Days Not Included</th>
<th>% Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13–17</td>
<td>NA</td>
<td>2</td>
<td>0</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>10–17</td>
<td>NA</td>
<td>2</td>
<td>0</td>
<td>75</td>
</tr>
<tr>
<td>3</td>
<td>11–14</td>
<td>January 14</td>
<td>0</td>
<td>2</td>
<td>100</td>
</tr>
<tr>
<td>4</td>
<td>13–17</td>
<td>January 15</td>
<td>2</td>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>5</td>
<td>10–16</td>
<td>NA</td>
<td>1</td>
<td>0</td>
<td>86</td>
</tr>
<tr>
<td>6</td>
<td>12–17</td>
<td>January 15</td>
<td>0</td>
<td>2</td>
<td>66.6</td>
</tr>
<tr>
<td>7</td>
<td>7–19</td>
<td>January 15</td>
<td>2</td>
<td>2</td>
<td>46</td>
</tr>
<tr>
<td>8</td>
<td>10–17</td>
<td>January 15</td>
<td>7</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>9</td>
<td>11–17</td>
<td>January 15</td>
<td>2</td>
<td>0</td>
<td>75</td>
</tr>
<tr>
<td>10</td>
<td>10–15</td>
<td>January 15</td>
<td>2</td>
<td>1</td>
<td>71</td>
</tr>
<tr>
<td>11</td>
<td>12–17</td>
<td>NA</td>
<td>2</td>
<td>2</td>
<td>66.6</td>
</tr>
<tr>
<td>12</td>
<td>12–15</td>
<td>January 15</td>
<td>0</td>
<td>2</td>
<td>100</td>
</tr>
<tr>
<td>13</td>
<td>11–16</td>
<td>NA</td>
<td>1</td>
<td>1</td>
<td>83</td>
</tr>
<tr>
<td>14</td>
<td>8–18</td>
<td>NA</td>
<td>5</td>
<td>0</td>
<td>55</td>
</tr>
<tr>
<td>15</td>
<td>10–16</td>
<td>January 15</td>
<td>1</td>
<td>0</td>
<td>86</td>
</tr>
<tr>
<td>16</td>
<td>10–16</td>
<td>January 15</td>
<td>1</td>
<td>0</td>
<td>86</td>
</tr>
<tr>
<td>17</td>
<td>10–15</td>
<td>January 15</td>
<td>1</td>
<td>0</td>
<td>86</td>
</tr>
<tr>
<td>18</td>
<td>10–17</td>
<td>NA</td>
<td>2</td>
<td>0</td>
<td>75</td>
</tr>
<tr>
<td>19</td>
<td>11–18</td>
<td>January 15</td>
<td>3</td>
<td>1</td>
<td>63</td>
</tr>
<tr>
<td>20</td>
<td>11–18</td>
<td>January 15</td>
<td>3</td>
<td>1</td>
<td>63</td>
</tr>
</tbody>
</table>

NA, not applicable.


† January 10–15.

‡ Calculated by dividing the total number of correct predicted fertile days by the total number of predicted fertile days, both correct and incorrect.

§ Duplicate applications in Apple iOS and Android.
The Pregnancy Panopticon

I feel watched
Sorry, Ellev
Our Findings

These have got to be the two dumbest people alive
Methods

• Static Analysis
  – JADX APK Decompiler
  – Android Studio
• Dynamic Analysis
  – MITM Proxy
• Kryptowire
Methods - JADX & Studio

I CAN HAZ SOURCE CODE?
Methods - MITM Proxy

SSL Added and removed here!
<table>
<thead>
<tr>
<th>App</th>
<th>Platform</th>
<th>Date Submitted</th>
<th>Threat Score</th>
<th>Security Issues</th>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pregnancy Calendar</td>
<td>Android</td>
<td>2017-06-28 16:41:33</td>
<td>81.4</td>
<td>- Can write to external storage, ◊ Loads code dynamically, ◊ Requests excessive permissions, $ Has in-app purchases, ◊ Integrates with social network, ◊ Makes a connection to foreign country</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>Pregnancy +</td>
<td>Android</td>
<td>2017-06-28 14:35:03</td>
<td>81.1</td>
<td>- Can access camera, ◊ Can access microphone, ◊ Can access contacts, ◊ Can send with SMS messages, ◊ Can write to external storage, ◊ Loads code dynamically, ◊ Requests excessive permissions, $ Has in-app purchases, ◊ Integrates with social network, ◊ Makes a connection to foreign country</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>Pink Pad Pro</td>
<td>Android</td>
<td>2017-06-28 14:36:15</td>
<td>78.6</td>
<td>- Can write to external storage, ◊ Loads code dynamically, ◊ Can obtain user/device specific information, ◊ Requests excessive permissions, ◊ Has in-app purchases, ◊ Integrates with social network, ◊ Exposes sensitive information, ◊ Makes a connection to foreign country, ◊ Integrates with ad network</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>WebMD Baby</td>
<td>Android</td>
<td>2017-05-16 12:35:19</td>
<td>78.6</td>
<td>- Can access camera, ◊ Can access contacts, ◊ Can write to external storage, ◊ Loads code dynamically, ◊ Requests excessive permissions, ◊ Integrates with social network, ◊ Exposes sensitive information, ◊ Makes a connection to foreign country, ◊ Integrates with ad network</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>Ovia Pregnancy</td>
<td>Android</td>
<td>2017-06-28 15:06:44</td>
<td>77.2</td>
<td>- Can write to external storage, ◊ Requests excessive permissions, ◊ Integrates with social network, ◊ Exposes sensitive information, ◊ Makes a connection to foreign country</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>Get Baby</td>
<td>Android</td>
<td>2017-06-28 14:59:04</td>
<td>75.1</td>
<td>- Can write to external storage, ◊ Loads code dynamically, ◊ Requests excessive permissions, ◊ Integrates with social network, ◊ Exposes sensitive information, ◊ Integrates with ad network</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>Eve</td>
<td>Android</td>
<td>2017-04-26 08:51:40</td>
<td>74.4</td>
<td>- Can access contacts, ◊ Can write to external storage, ◊ Loads code dynamically, ◊ Requests excessive permissions, ◊ Has in-app purchases, ◊ Integrates with social network, ◊ Exposes sensitive information, ◊ Integrates with ad network</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>BabyBump Pro</td>
<td>Android</td>
<td>2017-06-28 13:05:46</td>
<td>72.7</td>
<td>- Can write to external storage, ◊ Loads code dynamically, ◊ Can obtain user/device specific information, ◊ Requests excessive permissions, ◊ Integrates with social network, ◊ Makes a connection to foreign country</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
<tr>
<td>First Response</td>
<td>Android</td>
<td>2017-06-28 14:04:28</td>
<td>60.4</td>
<td>- Can access microphone, ◊ Can access contacts, ◊ Can write to external storage, ◊ Loads code dynamically, ◊ Requests excessive permissions, ◊ Integrates with social network, ◊ Makes a connection to foreign country</td>
<td>PDF Report, HTML Report, NAF HTML, JSON, PDF PRE</td>
</tr>
</tbody>
</table>
Code Execution and Content Injection

• HTML sent over plaintext and rendered directly.
• MITM Attacker could easily execute arbitrary javascript.
Account Hijacking

- Pinkpad
- WebMD Baby
- My Calendar
- The Bump
Personal Information Leaks

- Why does pinkpad send my location to the server every time it starts?
- Email, Name, Gender, Pregnancy status, etc.
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 18, 2016</td>
<td>Period Starts</td>
</tr>
<tr>
<td>Dec 21, 2016</td>
<td>Period Ends</td>
</tr>
<tr>
<td>Jan 18, 2017</td>
<td>Period Starts</td>
</tr>
<tr>
<td>Jan 18, 2017</td>
<td>Period Ends</td>
</tr>
<tr>
<td>Jan 18, 2017</td>
<td>Moods: Assertive</td>
</tr>
<tr>
<td>Jan 18, 2017</td>
<td>Weight: 300.0lb</td>
</tr>
<tr>
<td>Jan 18, 2017</td>
<td>Intercourse (Without Condom)</td>
</tr>
</tbody>
</table>
Third Party Tracking

THIRD-PARTY CONNECTIONS

THIRD-PARTY CONNECTIONS EVERYWHERE
Pin Locks

- 4 character limit
- Trivial to brute force
- No protection against root access
- “I forgot my code…”
- Probably shouldn’t rely on this
Files Not Deleted

• The Bump
• Upload pictures of pregnancy progress, ultrasounds, baby photos, etc.
• Once you delete the pictures...
• They aren’t really deleted but simply unlinked from your account. Still available on the public internet.
Permissions

• Location - Glow, WTE, Preg+, WebMD, Pinkpad, Baby Bump, Ovia Pregnancy, Ovia Fertility, Maya
• Contacts - Eve, Preg+, WebMD, BabyBump, Ovia Pregnancy
• Device ID - Glow, Eve, WTE, Pinkpad, BabyBump, The Bump
• Phone - Glow, Preg+, TheBump, Baby Bump
• SMS - Preg+
Certificate Pinning!

- Glow, Nurture, Eve, Clue all implement certificate pinning.
- My bank doesn’t even do this!
- Seems a little extra though...
Vendor Response

This is fine.
Vendor Response

• We contacted all of the vendors that had security problems
• WTE, WebMD, Preg+, Alt12, MyCalendar (both), Glow, Ptracker
• We received a response back from pTracker and Glow, who fixed the issues.
• Everyone else ignored or sent a form letter.
More Vendor Response

Kash heard back from everyone she emailed about privacy and policy issues, except for Everyday Health Inc. (What To Expect app) and alt12. Companies pay attention to journalists... or at least better understand what we’re telling them about.
What Can Hackers Do

• There are real threat models that none of these apps protect against.
• We need to convince app writers to take security and privacy issues more seriously.
These apps were useful for my first pregnancy...
But the privacy tradeoffs might not be worthwhile
Thanks!

- Thanks to Kryptowire for donating their analysis services.
- Thanks to Dave Choffnes and Jingjing Ren for help with Recon analysis.
- Thanks to Gizmodo Media and EFF for supporting this research.
- Thanks to Defcon, Nikita, and the Goons!
- Thanks to Ellev for inspiring this research!
Questions?

Kashmir Hill
kashmir.hill@gizmodomedia.com - @kashhill

Cooper Quintin
cooperq@eff.org - @cooperq
https://www.eff.org/wp/pregnancy-panopticon