



The Pregnancy Panopticon

Cooper Quintin, Staff Technologist, EFF

July 2017
Defcon 25

Table of Contents

Abstract	3
Methods	3
MITM Proxy	4
Jadx and Android Studio	4
Kryptowire	4
Security Issues	5
Code execution and content injection	5
Account Hijacking	6
Unencrypted Requests	6
Privacy Issues	6
Third Party Trackers	6
Pin Locks	8
Unauthenticated Email	8
Information Leaks	9
Files Not Deleted	9
Permissions	10
Conclusion	10
Acknowledgements	11
Appendix A - Permissions requested by each app	12
Appendix B. - Further Notes	13

Abstract

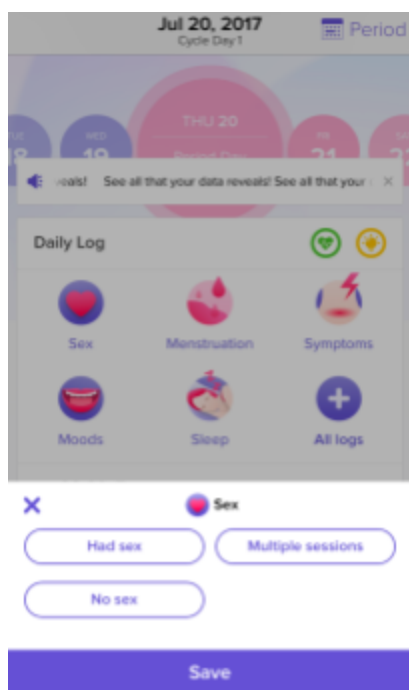


Fig 1. Some of the personal details logged by an application.

Women’s health is big business. There are a staggering number of applications for Android and iOS which claim to help people keep track of their monthly cycle, know when they may be fertile, or track the status of their pregnancy. These apps entice the user to input the most intimate details of their lives, such as their mood, sexual activity, physical activity, physical symptoms, height, weight, and more. But how private are these apps, and how secure are they in fact? After all, if an app has such intimate details about our private lives, it would make sense to ensure that it is not sharing those details with anyone, such as another company or an abusive family member. To this end, EFF and Gizmodo reporter Kashmir Hill have taken a look at some of the privacy and security properties of nearly twenty different fertility and pregnancy tracking applications. While this is not a comprehensive investigation of these applications by any means, we did uncover several privacy issues, some notable security flaws, and a few interesting security features in the applications we examined. We conclude

that while these applications may be fun to use, and in some cases useful to the people who need them, women should carefully consider the privacy and security tradeoffs before deciding to use any of these applications.

This document is a technical supplement to “[What Happens When You Tell the Internet You’re Pregnant](#)” published by Kashmir Hill on jezebel.com.

Methods

For this report we tested the following apps: Glow, Nurture, Eve, pTracker, Clue, What to Expect, Pregnancy+, WebMD Baby, Pinkpad, Flo, MyCalendar (Book Icon),¹ MyCalendar (Face Icon),² Fertility Friend, Get Baby, Babypod, Baby Bump, The Bump, Ovia, and Maya. Our methods involved dynamic analysis using the network man in the middle tool MITMProxy³ and ProxyDroid on a rooted Moto E Android phone running stock Android 4.4.4, static analysis

¹ com.popularapp.periodcalendar

² com.lbrc.PeriodCalendar

³ Man in the Middle Proxy - <https://mitmproxy.org/>

using the Jadx decompiler and Android Studio, and analysis using the Kryptowire Enterprise Mobile Management tool.

MITM Proxy

MITM Proxy is a proxy server which is able to intercept and decrypt HTTPS connections by installing a custom root certificate on the target device which is then used for all SSL connections. MITM Proxy is then able to decrypt and record a flow of plaintext and HTTPS traffic for inspection. MITM proxy can also be used to edit and replay requests. For this research we used MITM x`x`Proxy to inspect network traffic, review the APIs (Application Programming Interfaces) used by these applications, and determine which third parties are being contacted and what information is being sent to them.

Jadx and Android Studio

JADX⁴ is a decompiler for Android packages which is able to produce Java code that can be viewed and edited in the Android Studio programming environment. This technique was used to determine why and how certain permissions were used and other key information about the applications.

Kryptowire

Kryptowire⁵ is a proprietary Android application analysis platform which was generously donated to EFF for this research. Kryptowire was used to quickly scan a large number of applications for personal information leaks, common vulnerabilities, and excessive permissions.

Using Kryptowire, we were able to quickly discover issues in several applications, such as location leaks and bad programming practices including world readable preferences. We were also able to see where and how certain Android APIs were being used (for example, we found many applications requesting the name of the user's network operator) presumably for advertising purposes.

We were also able to quickly triage several applications that were not in our original set to determine whether they would require further manual analysis. Triageing these applications

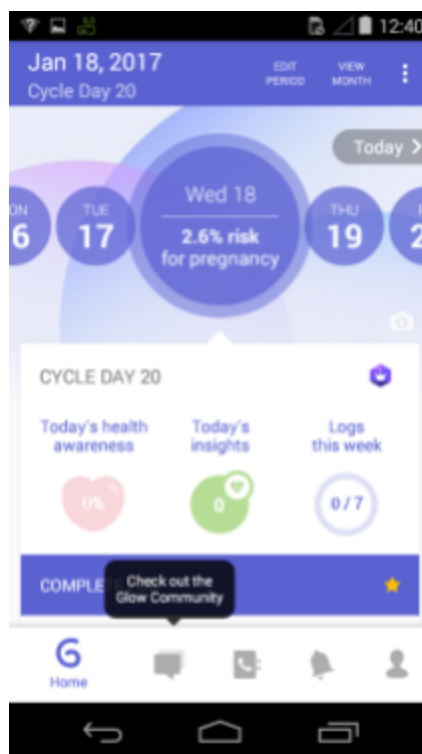


Fig 2. According to Glow the researcher has a 2.6% risk of getting pregnant. This seems high considering the researcher does not have a womb.

⁴ <https://github.com/skylot/jadx>

⁵ <http://www.kryptowire.com/>

would have taken several days of manual analysis, but using Kryptowire, we were able to do this work in a matter of minutes.

Security Issues

The “Glow” family of applications (Glow, Nurture, and Eve), as well as “Clue” all use certificate pinning—a technique which prevents someone with a fraudulently issued SSL certificate from intercepting traffic. This is a step not even taken by most banking apps, and it is certainly a good way to protect against a certain class of attack. Unfortunately, this same property prevents us from inspecting the HTTPS traffic of these apps with MITM Proxy, meaning we are unable to do further dynamic analysis on these applications.

Certificate pinning is a desirable—if esoteric—security feature to include. On the other hand, none of the apps examined support two-factor authentication, which may have been a more practical step for securing users’ information against common attacks.

Code execution and content injection



Fig 3. Some of the application icons are less subtle than others.

Several apps (What to Expect, WebMD Baby, Pregnancy+, and both apps named MyCalendar) make unencrypted requests for HTML content which were then displayed to the user. This raises the possibility of a man in the middle code execution attack against these applications. None of the applications appears to do any sanitizing of the input that they receive from the unencrypted HTML request.

Both MyCalendar applications fetch advertisements meant for display over an unencrypted connection, raising the further possibility of a man in the middle content injection. What’s more, MyCalendar (Face Icon) makes an unauthenticated HTTPS request to the ajax.googleapis.com CDN to get a copy of the jQuery library. An attacker who can create a self signed certificate for ajax.googleapis.com could inject their own copy of the jQuery library in it’s place. This could potentially allow for the possibility of code execution within the application, and even account takeover, if JQuery is used to handle authentication at all, though the researcher has not confirmed this.

Account Hijacking

Pinkpad, WebMD Baby, The Bump, and MyCalendar (Book Icon) send unencrypted user authentication cookies over the network. This means that a man in the middle attacker could easily take over a user's account. This is an extremely severe security flaw. No application should be making any unencrypted requests when [free SSL certificates](#) are available, and certainly not requests containing user authentication tokens.

Unencrypted Requests

What to expect, Eve, Pregnancy+, pTracker, WebMD Baby, Pinkpad, and both MyCalendar apps make plaintext HTTP requests to app servers and third party servers. Of those, pTracker, and MyCalendar (Book Icon) only make third party requests unencrypted while MyCalendar (Face Icon), Eve, and Pregnancy+ only make unencrypted requests to first party servers. This issue has been fixed in Eve as of this report.

As we stated above, unencrypted requests should be considered harmful due to the high probability of data leakage, code execution, and account hijacking. The industry best practice would be to not ever send any unencrypted data to another server and we recommend that all applications do this immediately.

Privacy Issues

Third Party Trackers

When an application makes an internet connection to a domain other than one owned by the company that made it, this is called a Third Party connection. Third party connections are often used for analytics, content delivery and advertising. Some common third parties that applications connect to include Doubleclick, Google, Facebook, Crashlytics, and Amazon. All third party connections have the ability to uniquely identify your phone and track which applications you are using on it (and sometimes more detailed information as well). Third party connections may purposefully or accidentally reveal sensitive information about the user. When found in conjunction with applications that record intimate details about our health and sex life, this can be especially troubling.

Almost all of the applications we tested make requests to third party servers, the notable exception being Fertility Friend. The application with the largest number of third party connections is The Bump, which connects to over 18 different third party domains. The most popular third party services are Google and Facebook, which both appear in 15 different

applications, followed by Doubleclick (owned by Google) which appears in 13 different applications, and Crashlytics (owned by Google) in 11 different applications.

Glow and Eve were both observed sending the phone's IMEI (a permanent serial number for the device) to the AppsFlyer third party server. The IMEI can be used to uniquely identify a device across multiple apps even if the phone is factory reset or a new operating system is installed. Due to the massive privacy problems this presents, many developers have switched to using the "mobile advertising id," which Google and Apple both support and which can be changed by the user. We reported this issue to Glow (which also makes Eve) and were informed that it has been fixed in the latest version.

We observed that "Flo" sends the following data in a request to the Facebook Graph API:

```
custom_events_file: [{
  "_ui": "unknown", "_session_id": "7480e02d-1eb6-4216-bfaf-xxxx
  xxxx",
  "_eventName": "SESSION_FINISHED_FIRST_LAUNCH", "graph": "true"
  ,
  "event_added": "true", "_logTime": 1484779886,
  "Menstruation_changes": "true"
}]
```

Apparently this API is used for analytics and conversion tracking by the developer. According to Facebook:

Facebook does not share any app event data sent on your behalf to advertisers or other third parties, unless we have your permission or are required to do so by law.

It is unclear how much privacy protection this statement actually offers. Facebook also stores this data along with the user's advertising ID, mentioned above, meaning this data could potentially be linked to data from other apps as well.

Pin Locks

pTracker, Clue, MyCalendar (Book), MyCalendar (Face), Fertility Friend, Pinkpad, Flo, Maya, and WebMD Baby all support a PIN code for access. While this is better than nothing for protecting data from a local attacker (e.g. an abusive partner or guardian), it falls far short of offering effective security.

The pin code does not appear to offer any encryption, thus any attacker who can gain root access to the phone would be able to extract data from the applications. Additionally, none of the pin codes have any limit on the number of tries or any sort of delay, and most of them limit the pin to 4 digits, making them fairly easy targets on which to perform a brute force attack. Maya will email a reset code to your email account, which is presumably also accessible from the user's phone, making the pin lock useless. MyCalendar (Book Icon) stores backup data in plaintext on the SD card, rendering the pin code entirely useless. Therefore, we conclude that these pin codes are unreliable for the purpose of ensuring data security.

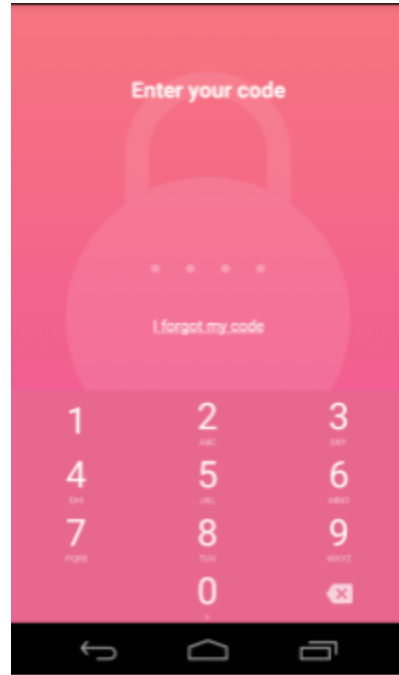


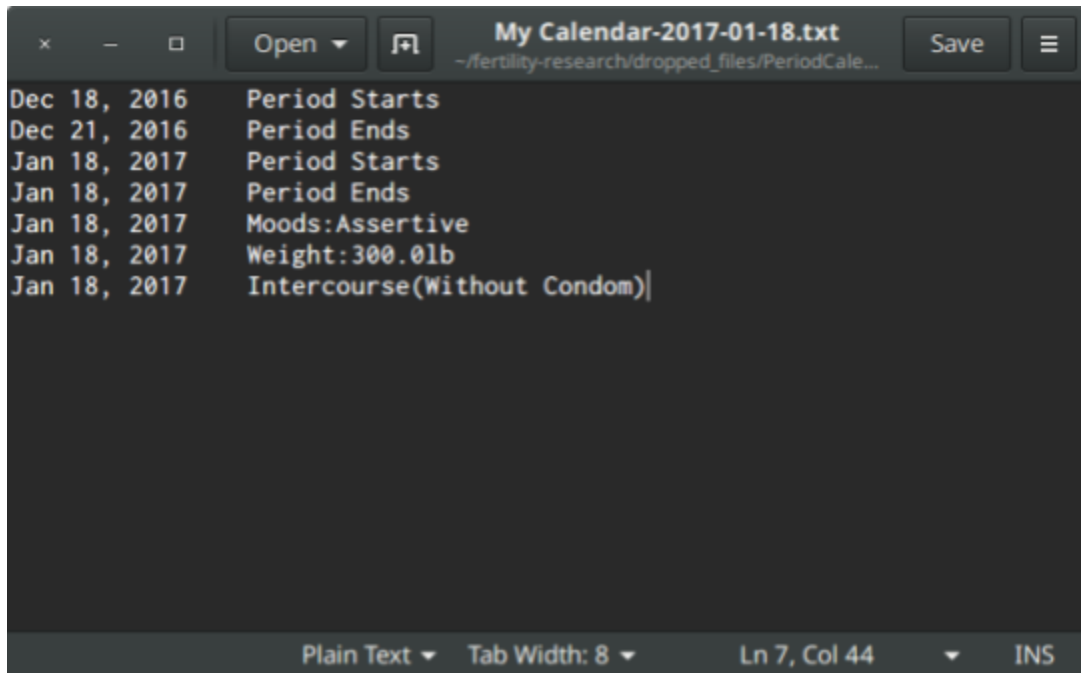
Fig 4. Pin Code entry screen

Unauthenticated Email

What To Expect has several API endpoints which could allow a malicious actor to send a large number of emails to an email address of their choice. While the attacker does not get to choose the contents of the mail, they could still flood a person's inbox with a large number of unwanted emails, causing a nuisance.

The What to Expect API also allows one to sign up for a large number of mailing lists without confirming the receiving address. Using this, one could sign their friends up for several dozen mailing lists without any confirmation.

Information Leaks



```
My Calendar-2017-01-18.txt
~/fertility-research/dropped_files/PeriodCale...

Dec 18, 2016   Period Starts
Dec 21, 2016   Period Ends
Jan 18, 2017   Period Starts
Jan 18, 2017   Period Ends
Jan 18, 2017   Moods:Assertive
Jan 18, 2017   Weight:300.0lb
Jan 18, 2017   Intercourse(Without Condom)|

Plain Text ▾ Tab Width: 8 ▾ Ln 7, Col 44 ▾ INS
```

Fig 5. MyCalendar data retrieved from the SD Card

We found several information leaks during the course of our research, some of which were quite disturbing. The MyCalendar app, for example, writes a log of everything that you enter into it into a text file which is stored on the SD card, as seen in Figure 4. The fact that this is written to the SD card means that any other application or person with access to the user’s phone could trivially read it and learn detailed personal information.

The Alt12⁶ family of applications (Pinkpad and Baby Bump) were both found to send the user’s precise GPS coordinates to the alt12 application server every time the application was opened. The applications give no indication to the user that this is happening. We can only guess as to why the application does this, perhaps for the purposes of geo-targeted advertising. Glow, Pregnancy+, What to Expect, and WebMD Baby were all found to access the user’s location. Regardless of why the location is accessed and recorded, it is an extremely subtle and disturbing invasion of privacy.

Files Not Deleted

One application we tested, The Bump, had a feature which allowed users to upload a picture of themselves while pregnant (called a “belly photo”) or a photo of their children. We discovered that deleting these pictures in the application did not cause the pictures to be removed from the

⁶ <https://www.alt12.com/>

server, leaving them available to be accessed publicly. This is, of course, unexpected behavior and could be a severe issue if someone using this application uploaded a photo including personal or private information that they later wished to remove.

Permissions

We also performed a cursory examination of the permissions required by each application. Get Baby is unique in that it requires zero permissions for use. pTracker requires only one permission, and most of the applications require only 2 or 3 permissions. On the opposite end of the spectrum, Pregnancy+ requires 9 different permissions. It's also important to note that the number of permissions does not directly correlate with the degree of privacy an application offers.

Most of the apps request the SD card permission, which is used to store data, cache, and photos from the app and is generally harmless. Several of the applications, however, request location permission to determine fine-grained location information. The researcher is unable to determine how this might be used other than to enable geo-targeted ads. The dangers of geo-targeted ads are outside the scope of this paper, but there have been some stunning demonstrations of [how they can be used maliciously](#).

The Device ID permission is used by Glow, Eve, What to Expect, and Pinkpad to get the IMEI⁷ of the device. This is most likely used for advertising. Since the IMEI is unchangeable under normal operation, it is a very intrusive method of tracking, allowing advertisers to continue tracking a user even if they factory reset their devices. For this reason, Google has discouraged the use of IMEI for advertising. Eve has fixed the issue as of this report.

Conclusion

The number of security and privacy issues that we discovered in just this cursory look at the few most popular applications could lead one to a pretty grim view of women's health applications. Certainly several of the applications had severe privacy and security issues and could not be recommended.

Our research here is not exhaustive, and there are still many avenues of research in these applications left unexplored. For example, Elvie sends the user's password to the server as an unsalted SHA1 hash. If passwords are stored this way, they would be easy to crack if someone were to get ahold of the hashes. Even worse, Maya appears to store the user's password as plaintext, which is emailed to the user when they request a password reset.

On the other hand, some of the applications did surprisingly well on our tests. Fertility Friend, for example, makes no third party server contacts (except for YouTube for viewing tutorials) and

⁷ International Mobile Equipment ID - A hardware serial number uniquely identifying a phone.

has no obvious security flaws that we have found. Clue seems to be relatively secure and has a well-implemented feature for sharing the user's cycle with others. On the other hand, many of these applications appear to have been written extremely quickly, consisting of no more than a calendar, some code to calculate averages, and an advertising library. These applications aren't usually complex enough to have any serious security vulnerabilities, but they shouldn't be relied on for medical advice, and one should consider how much personal information could be sent to third parties through their use.

Acknowledgements

Huge thanks to Kryptowire for donating their analysis tools. Thanks to EFF and Gizmodo media for funding this research. Thanks to Kashmir Hill and Elev for the inspiration and co-research. Thanks to A for inspiration and support.

Appendix A - Permissions requested by each app

App	SD Card	Purchases	Identity	Location	Phone	Device ID	Contacts	sms	Camera	Wifi
Period Tracker	✓									
Glow	✓	✓	✓	✓	✓	✓				
Nurture	✓	✓	✓							
Clue	✓		✓							✓
Eve	✓	✓	✓			✓	✓			
What to expect	✓		✓	✓		✓				✓
Pregnancy+	✓	✓	✓	✓	✓		✓	✓	✓	✓
Webmd Baby	✓			✓			✓		✓	✓
Pinkpad	✓	✓	✓	✓		✓				✓
Flo	✓									✓
MyCalendar (Book)	✓		✓							✓
MyCalendar (Face)	✓	✓								
Fertility Friend	✓	✓								
Get baby										
Babypod	✓		✓							✓
BabyBump	✓		✓	✓	✓	✓	✓			✓
Ovia Pregnancy	✓		✓	✓			✓			✓
Ovia Fertility	✓			✓						✓
The Bump	✓				✓	✓			✓	✓
Maya	✓	✓		✓					✓	

Appendix B. - Further Notes

App	Unencrypted Requests	Third Party Requests	Notes
Period Tracker	third party	Apsalar, Doubleclick, Google, Google-Analytics	Supports pin lock
Glow	none	Crashlytics, Appsflyer, Google, Ravenjs, Cloudfront, Facebook	Appears to use certificate pinning
Nurture	none	Crashlytics, Appsflyer, Google, Ravenjs, Cloudfront, Facebook	Made by Glow, appears to use cert pinning
Clue	none	Amplitude, Branch.io, Lean plum, Crashlytics, Facebook, Flurry	Good privacy policy, lower number of third parties, supports pin lock
Eve	first party	Facebook, Crashlytics, Lyr8, Appsflyer, Branch.io	Made by the same company that makes Glow, some certificate pinning in use possibly, responded and fixed security issues
What to expect	first and third party	Brightcove, 2o7, Doubleclick, Facebook, Google-Analytics, Scorecard research, Google	Opts users into two different mailing lists, can't use + in email when registering
Pregnancy+	first party	Google-Analytics, Crashlytics, Doubleclick, Facebook, Google, Flurry	
Webmd Baby	first and third party	Facebook, Demdex, Crashlytics, Appboy, Scorecardresearch, Doubleclick	Supports pin lock, doesn't allow + in email address
Pinkpad	first and third party	Flurry, Facebook, Google-Analytics, Google, Amazon, Newrelic, Cloudfront	Supports pin lock, shares GPS coordinates with server on startup

App	Unencrypted Requests	Third Party Requests	Notes
Flo	none	Facebook, Flurry, Crashlytics, Google	Supports pin lock
MyCalendar (Book)	first party	Crashlytics, Doubleclick, Google, Google-Analytics, Facebook	Supports pin lock
MyCalendar (Face)	third party	Crashlytics, Google, Doubleclick, MoPub, Facebook, AdMarvel, Rubicon project, TapSense, Amazon, BlueKai, others	Supports pin lock
Fertility Friend	None	None	Loads tutorials from youtube but opt-in
Get Baby	none	Google, Doubleclick	
Babypod	n/a	n/a	No network connection
BabyBump	None	Facebook, Google, Flurry, Localytics, Crashlytics	Shares GPS coordinates with server on startup
Ovia Pregnancy	Third party	Facebook, Google, Scorecard, Flurry, Crashlytics, Optimizely, Moatads, AllFont.net	
Ovia Fertility	None	Facebook, Google, Scorecard, Flurry, Crashlytics, Optimizely	
The Bump	First and third party	Scorecard, GPSoneXtra, Facebook, Amazon, Advertising.com, Demdex, Nexac, Rlcdn, Addthis, eAccelerator, Bluekai, Doubleclick, Segment, Moatads, Google, Mixpanel, Rubicon, MathTag, and more.	Fails to remove deleted files from server, Leaks authentication tokens over HTTP
Maya	None	Facebook, Google, Crashlytic, Clevertap	Supports pin Lock, passwords stored in plaintext