Tracking the Period Trackers

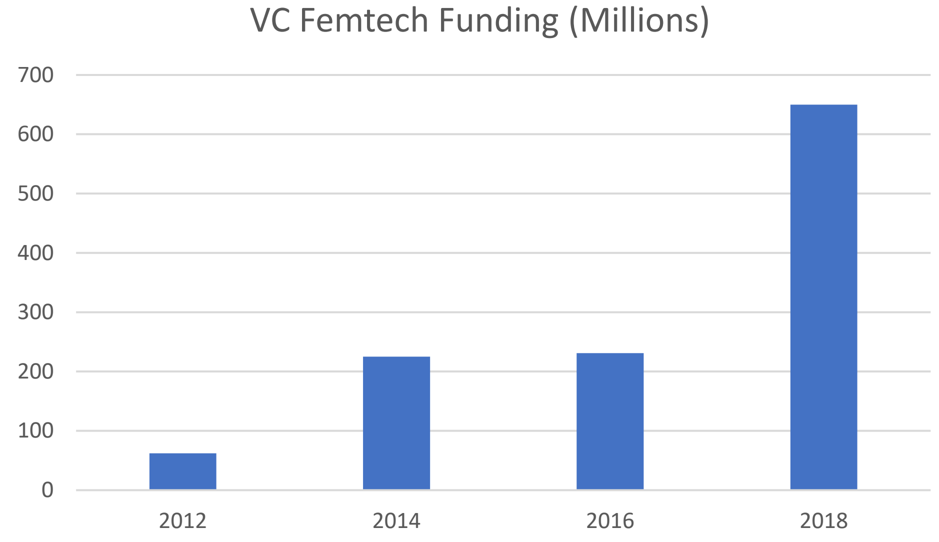
Wendy Edwards

Jacqueline Xavier

Summercon 2019

Femtech

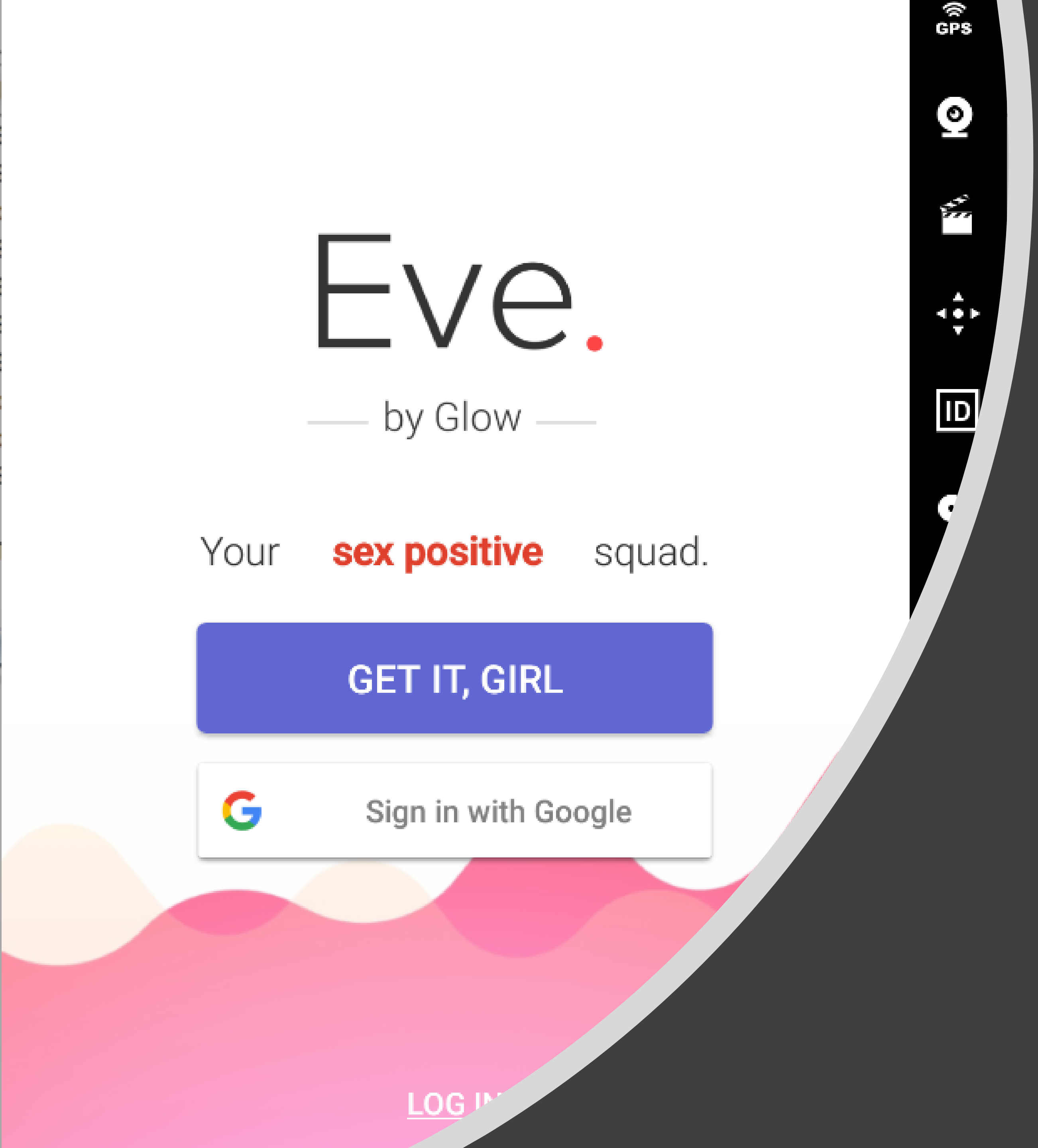
- Software, diagnostics, products or services that leverage technology to improve women's health (including period trackers)
- VC investment could reach $1 billion this year



https://techcrunch.com/2019/04/03/femtechs-billion-dollar-year/

Android Period Tracker Apps

- Clue Period Tracker (Biowink)
- Eve Period Tracker (Glow)
- My Calendar (SimpleInnovation)
- Ovia Fertility (Ovia Health)
- Period Tracker (GP International)
- Period Tracker (Amila)
- Period Tracker (Simple Design Ltd)
- Spot On (Planned Parenthood)
- Period Tracker Flo (Flo)
- Period Tracker (Leap Fitness Group)



But Is There a Privacy-Positive Squad?

Android Apps and Privacy

Transmitting identifying information to third parties (often advertisers)

- Some apps send permanent identifiers (e.g., IMEI) along with advertising ID (https://blog.appcensus.mobi/2019/02/14/ad-ids-behaving-badly/)

Dangerous permissions (Location, SMS, Storage, etc)

General security holes

Analyzing Android Apps

Static

- Decompile and analyze the code without executing
- Can sometimes catch errors that don’t appear in dynamic analysis

Dynamic

- Actually execute code
- Can capture and examine network traffic

Existing Resources

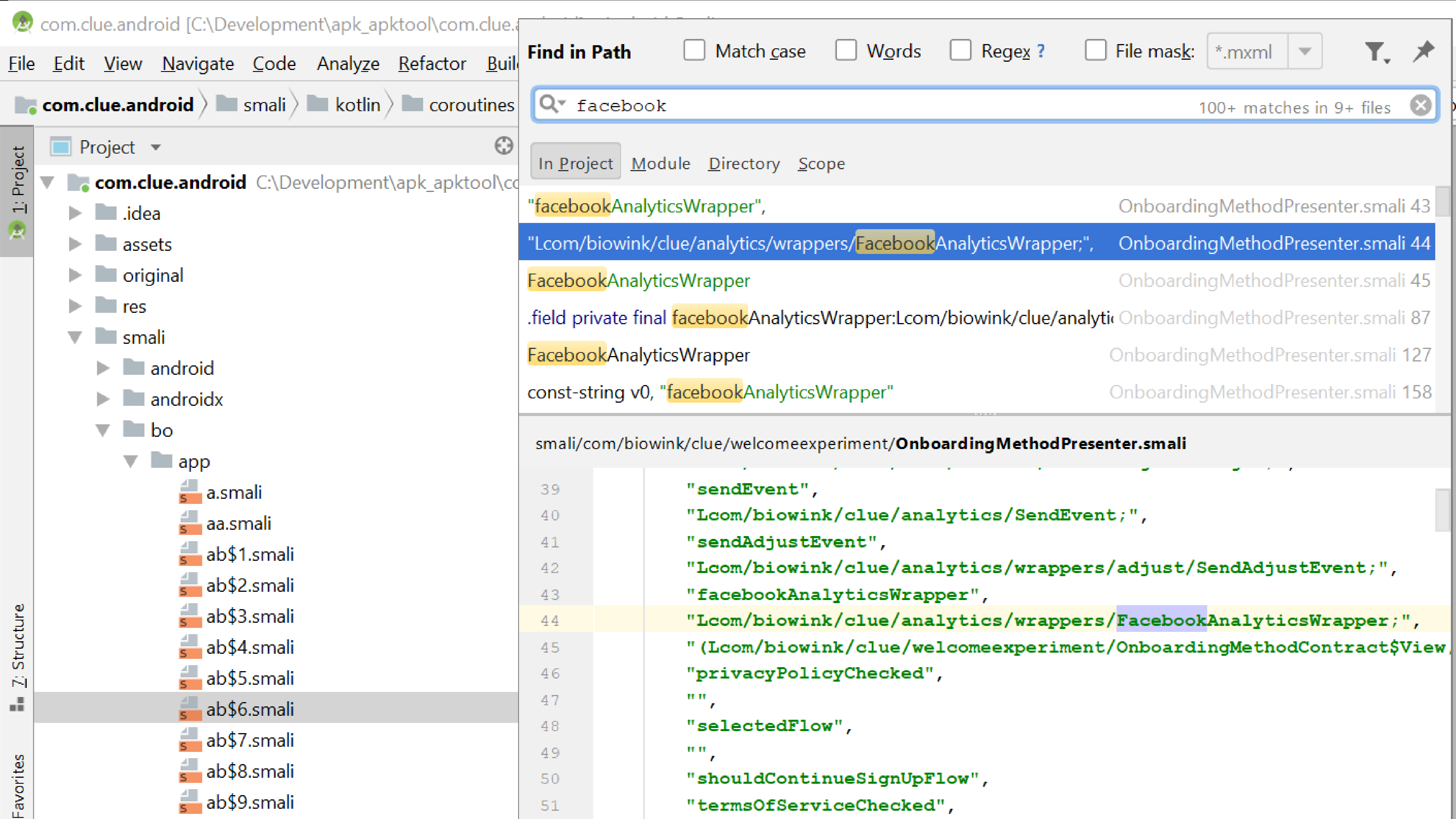
- VirusTotal (https://www.virustotal.com/gui/home/upload)
  - Online resource aggregating numerous antivirus and scan engines online
  - Includes Droidy, a sandbox for Android
- AppCensus (https://search.appcensus.io)
  - Searchable database of Android apps that have been dynamically tested for private and personally identifying information
- Exodus (https://reports.exodus-privacy.eu.org)
  - Another searchable database with reports on Android apps and privacy
- Other static analysis tools
  - ImmuniWeb (https://www.immuniweb.com/)

Static Analysis

Automated tools, e.g. VirusTotal

Decompile APK with APKTool (https://ibotpeaches.github.io/Apktool/)

View, recompile, and sign code with Android Studio(IDE) (https://developer.android.com/studio)



```
facebook                                            100+ matches in 9+ files
```

```
"facebookAnalyticsWrapper",                                                   OnboardingMethodPresenter.smali 43
"Lcom/biowink/clue/analytics/wrappers/FacebookAnalyticsWrapper;",            OnboardingMethodPresenter.smali 44
FacebookAnalyticsWrapper                                                      OnboardingMethodPresenter.smali 45
.field private final facebookAnalyticsWrapper:Lcom/biowink/clue/analyti      OnboardingMethodPresenter.smali 87
FacebookAnalyticsWrapper                                                      OnboardingMethodPresenter.smali 127
const-string v0, "facebookAnalyticsWrapper"                                   OnboardingMethodPresenter.smali 158
```

smali/com/biowink/clue/welcomeexperiment/**OnboardingMethodPresenter.smali**

```
        "sendEvent",
        "Lcom/biowink/clue/analytics/SendEvent;",
        "sendAdjustEvent",
        "Lcom/biowink/clue/analytics/wrappers/adjust/SendAdjustEvent;",
        "facebookAnalyticsWrapper",
        "Lcom/biowink/clue/analytics/wrappers/FacebookAnalyticsWrapper;",
        "(Lcom/biowink/clue/welcomeexperiment/OnboardingMethodContract$View
        "privacyPolicyChecked",
        "",
        "selectedFlow",
        "",
        "shouldContinueSignUpFlow",
        "termsOfServiceChecked",
```

What to Look For

Manifest (AndroidManifest.xml)

- Package name and appID
- Components
- Permissions
- Hardware and software components required by app

Interesting strings

- Advertising IDs
- URLs

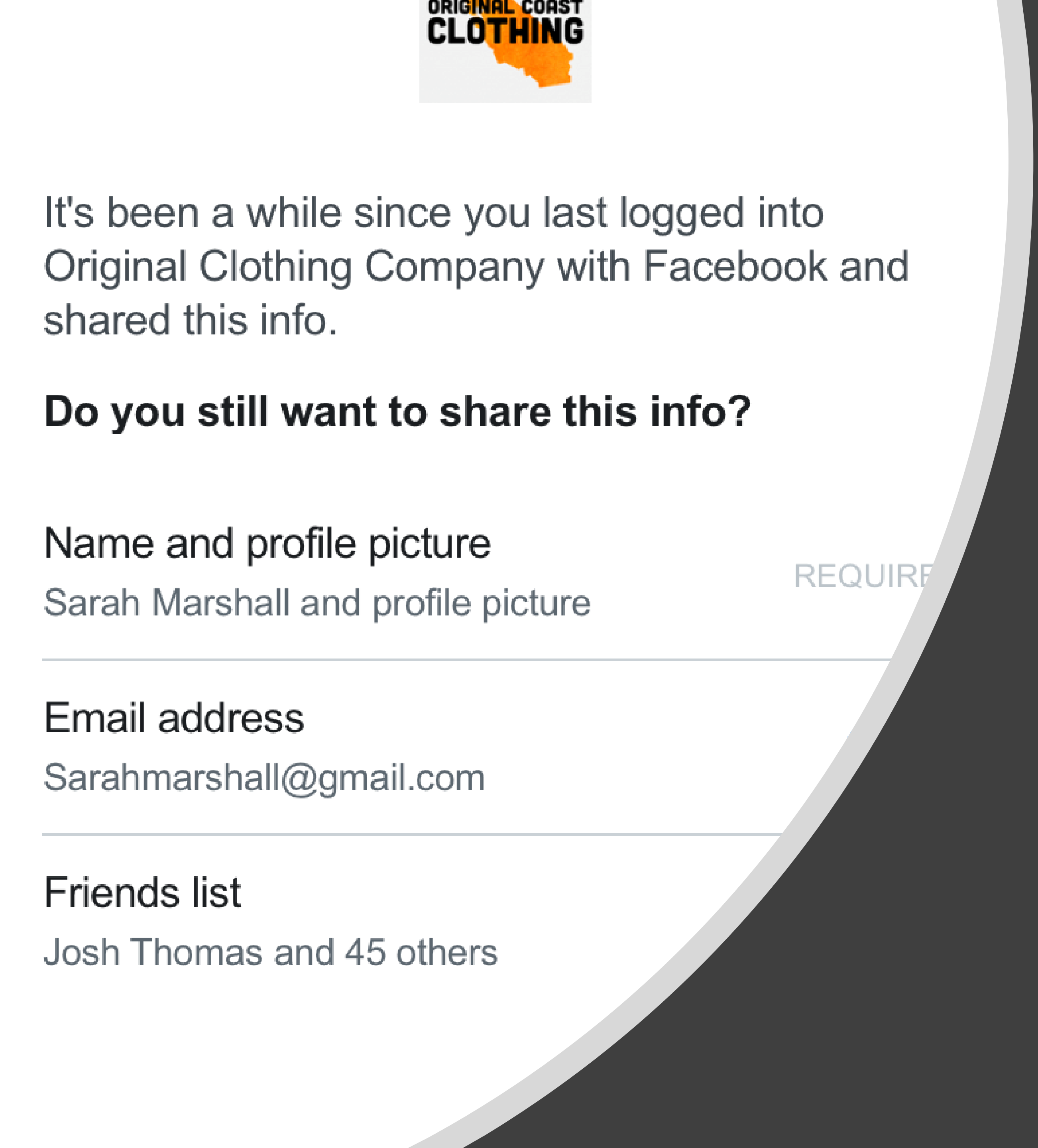
External libraries

Single Sign-On (SSO) Authentication

Common approaches are OAuth, OpenID Connect (OIDC), and Security Assertion Markup Language (SAML)

With Android apps, Google and Facebook are often used as the Identity Provider (IdP). The application itself is called the Service Provider (SP)

The IdP can send user information as part of the login process (e.g., Facebook prompting for permission to send data)



It's been a while since you last logged into Original Clothing Company with Facebook and shared this info.

Do you still want to share this info?

Name and profile picture
Sarah Marshall and profile picture
REQUIRE

Email address
Sarahmarshall@gmail.com

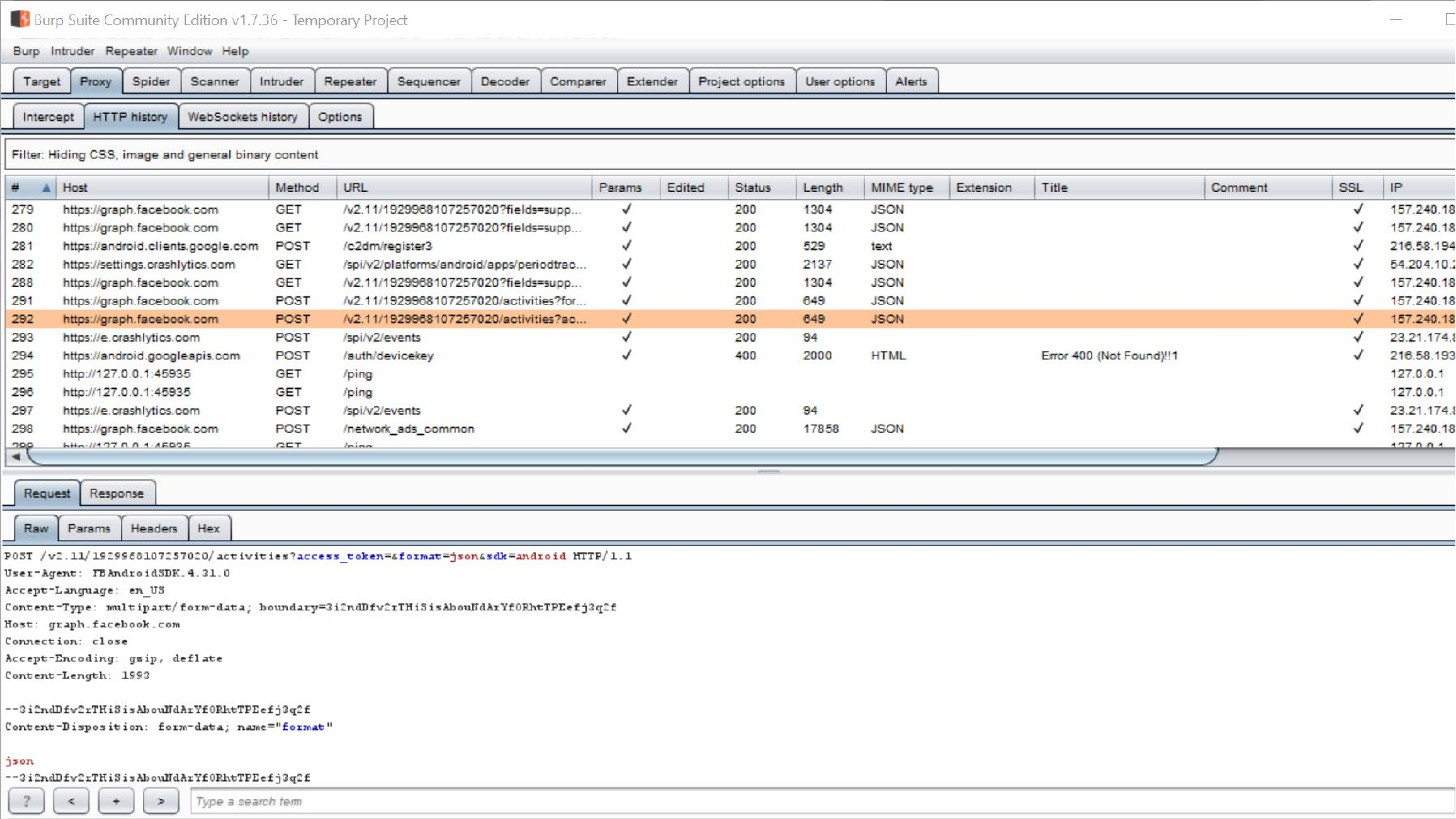
Friends list
Josh Thomas and 45 others

Facebook Permissions

Can share a lot of data

Analyzing Network Traffic

- Use Android emulator with rooted image. Genymotion has a free personal edition (https://www.genymotion.com/fun-zone/) and there are others, e.g., Bluestacks and Android Studio
- Intercepting Proxy
  - BurpSuite Community Edition (https://portswigger.net/burp/communitydownload)
  - Charles (https://www.charlesproxy.com/)
  - MitmProxy (https://mitmproxy.org/)
  - Fiddler (https://www.telerik.com/fiddler)


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex
? < + >
Type a search term

Filter: Hiding CSS, image and general binary content

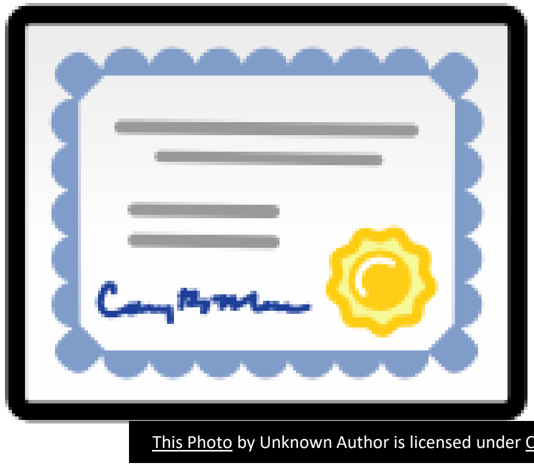
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
279	https://graph.facebook.com	GET	/v2.11/1929968107257020?fields=supp...	✓		200	1304	JSON				✓	157.240.18
280	https://graph.facebook.com	GET	/v2.11/1929968107257020?fields=supp...	✓		200	1304	JSON				✓	157.240.18
281	https://android.clients.google.com	POST	/c2dm/register3	✓		200	529	text				✓	216.58.194
282	https://settings.crashlytics.com	GET	/spi/v2/platforms/android/apps/periodtrac...	✓		200	2137	JSON				✓	54.204.10.2
288	https://graph.facebook.com	GET	/v2.11/1929968107257020?fields=supp...	✓		200	1304	JSON				✓	157.240.18
291	https://graph.facebook.com	POST	/v2.11/1929968107257020/activities?for...	✓		200	649	JSON				✓	157.240.18
292	https://graph.facebook.com	POST	/v2.11/1929968107257020/activities?ac...	✓		200	649	JSON				✓	157.240.18
293	https://e.crashlytics.com	POST	/spi/v2/events	✓		200	94					✓	23.21.174.8
294	https://android.googleapis.com	POST	/auth/devicekey	✓		400	2000	HTML		Error 400 (Not Found)!!1		✓	216.58.193
295	http://127.0.0.1:45935	GET	/ping										127.0.0.1
296	http://127.0.0.1:45935	GET	/ping										127.0.0.1
297	https://e.crashlytics.com	POST	/spi/v2/events	✓		200	94					✓	23.21.174.8
298	https://graph.facebook.com	POST	/network_ads_common	✓		200	17858	JSON				✓	157.240.18
299	http://127.0.0.1:45935	GET	/ping										127.0.0.1

```
POST /v2.11/1929968107257020/activities?access_token=&format=json&sdk=android HTTP/1.1
User-Agent: FBAndroidSDK.4.31.0
Accept-Language: en_US
Content-Type: multipart/form-data; boundary=3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
Host: graph.facebook.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 1993

--3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
Content-Disposition: form-data; name="format"

json
--3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
```

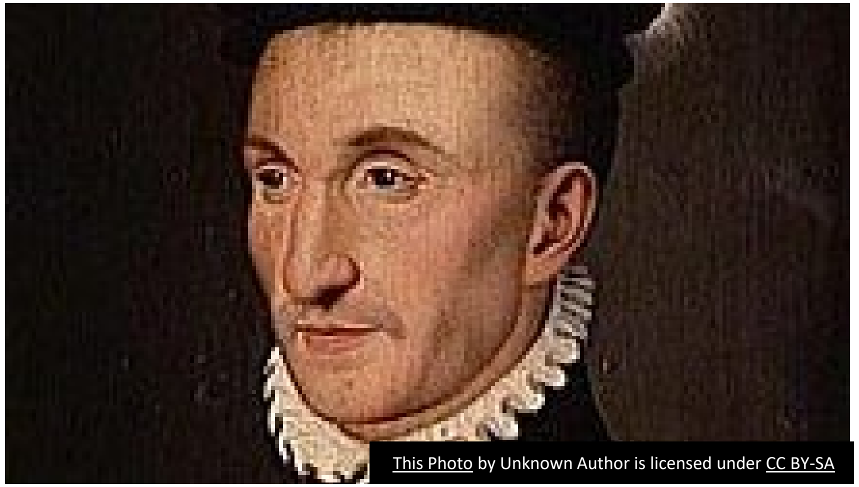
Certificate Pinning



- We can generate a cert from the proxy software and tell our emulator to trust it, but that doesn’t always work.
- Why not? Certificate pinning!
- Instead of just trusting any cert like we’d like, app checks against hard-coded cert values.

Bypassing Certificate Pinning

- Will no one rid me of this meddlesome code?
- FRIDA (https://www.frida.re/)
  - Running script live
  - Modifying code with Objection (https://github.com/sensepost/objection)
- Decompiling and replacing code



Findings

Fairly run-of-the mill security issues

- Unencrypted external storage, weak encryption, unparameterized SQL statements

Permissions

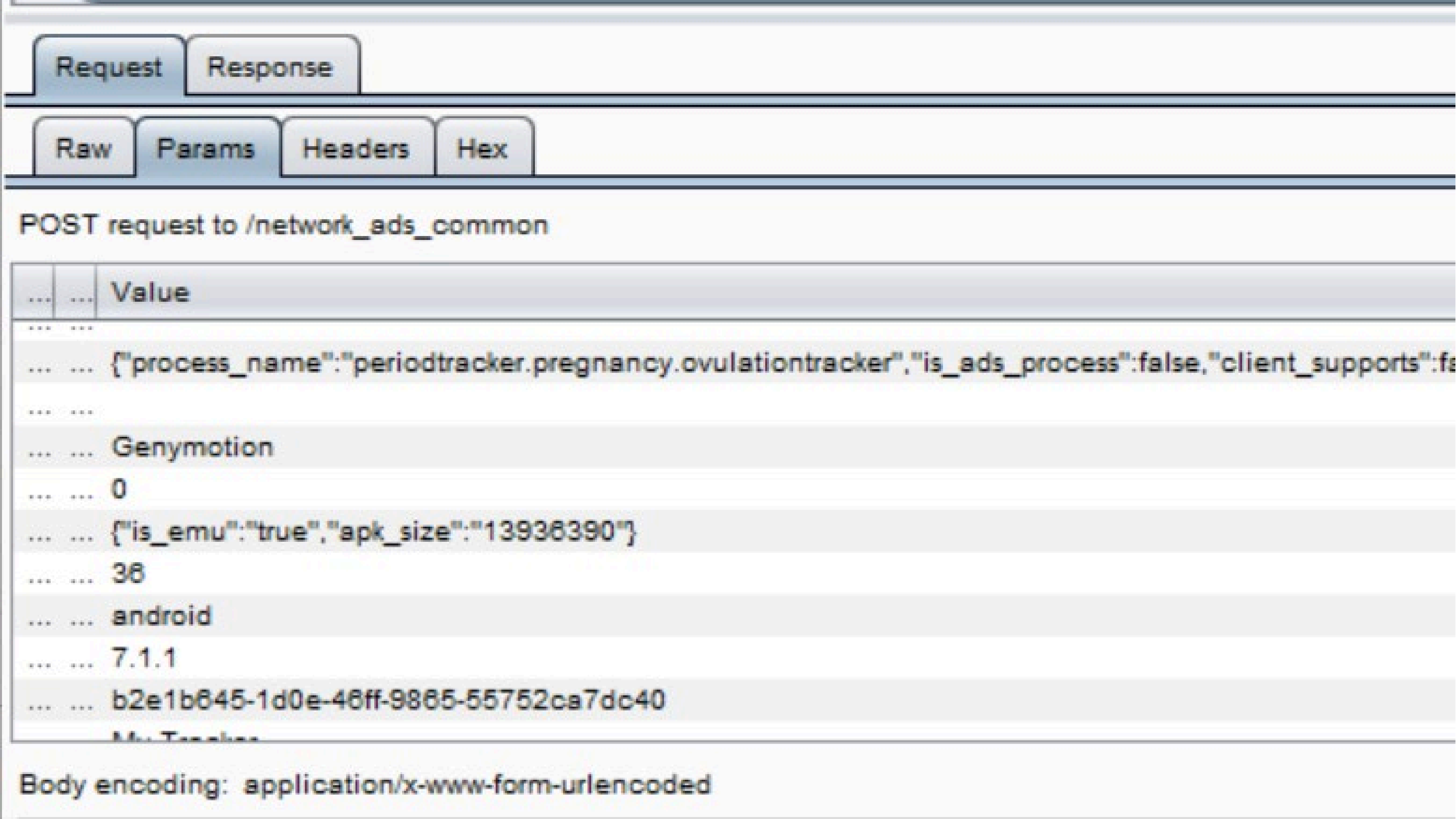
- Read/write SD storage was common
- Get accounts (Eve, Period Calendar, Leap Period Tracker)
- Read contacts (Ovuline)
- Start silently (Clue)

Trackers

- All had trackers
- Flo had only one (Google)
- Period Tracker (GP International) won the prize with 19 trackers

Information Commonly Sent

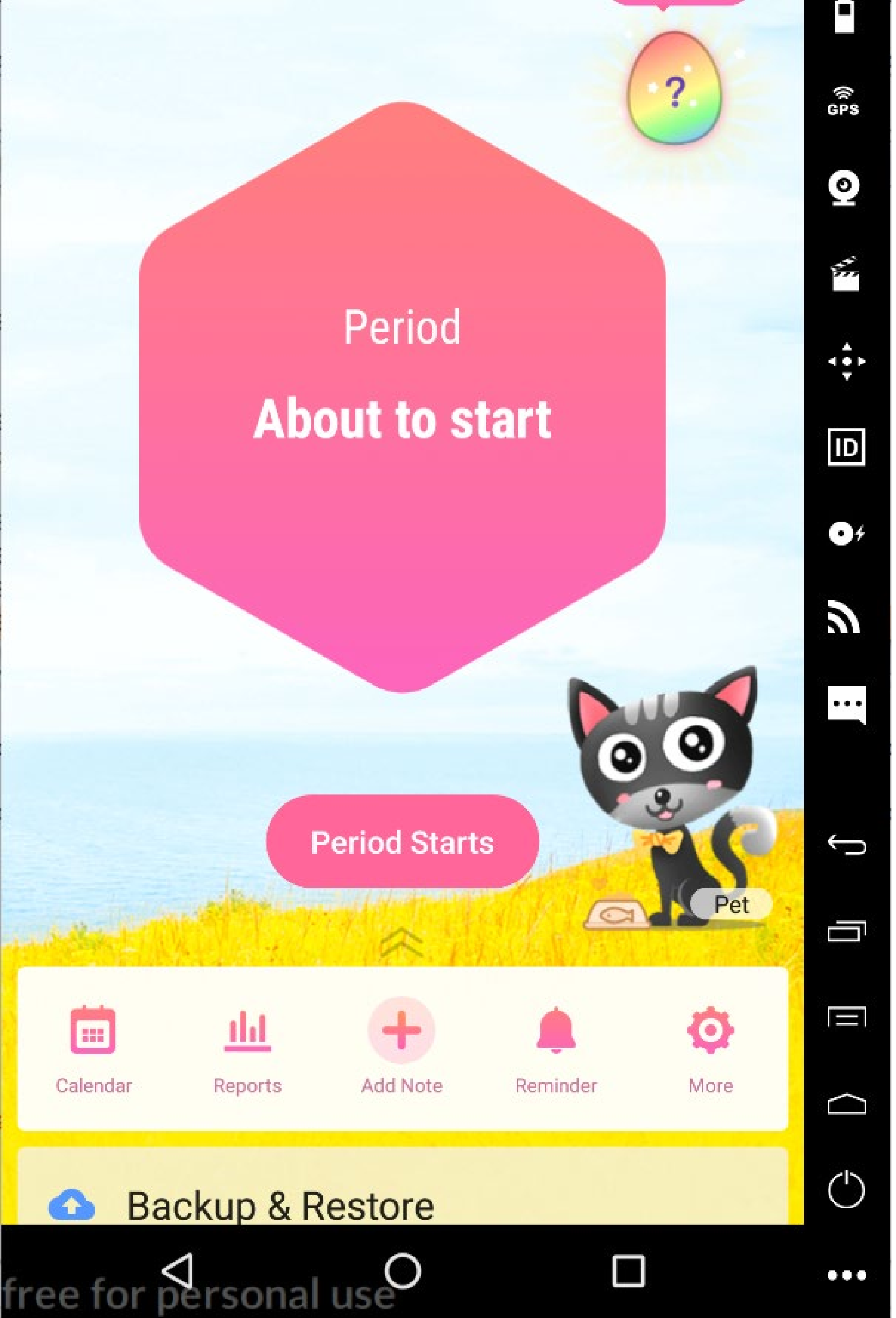
- Device fingerprint
- Advertising ID
- Phone information
  - Phone make and model
  - Android build
- Anon ID



POST request to /network_ads_common

...	...	Value
...	...	
...	...	{"process_name":"periodtracker.pregnancy.ovulationtracker","is_ads_process":false,"client_supports":fa
...	...	
...	...	Genymotion
...	...	0
...	...	{"is_emu":"true","apk_size":"13936390"}
...	...	36
...	...	android
...	...	7.1.1
...	...	b2e1b645-1d0e-46ff-9865-55752ca7dc40
		My Tracker

Body encoding: application/x-www-form-urlencoded

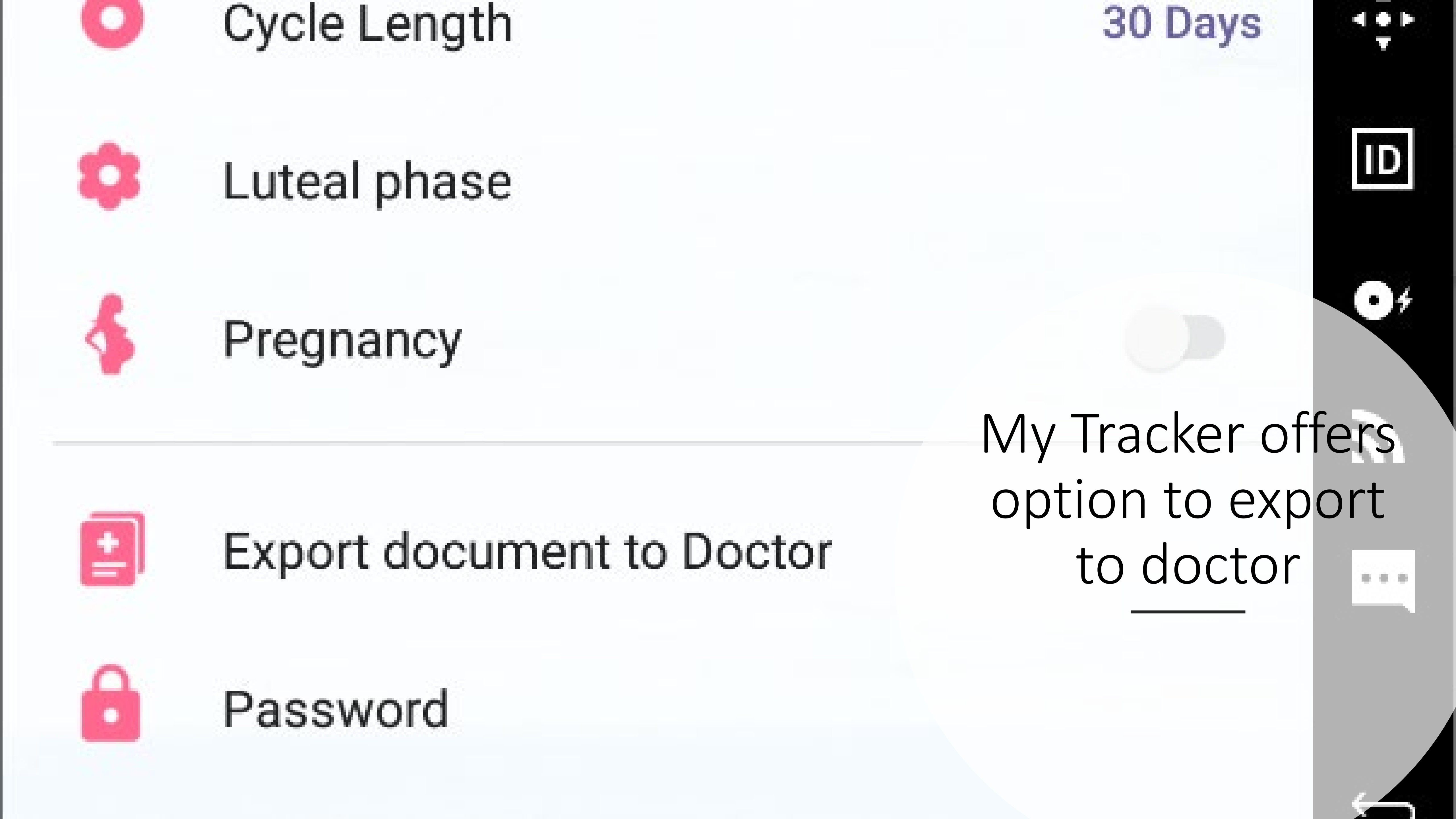


In-App Promotions

- Other apps by same company
- In-app purchases like “pets”

Healthcare Perspective: Why is this important?

- If doctors request that a patient use an app as part of their care plan, and these apps leak sensitive data, this is then **patient information** that is being leaked.
- But this information is currently not protected under HIPAA, which has strict guidelines for security and privacy regarding patient data.



Cycle Length 30 Days

Luteal phase

Pregnancy

Export document to Doctor

Password

My Tracker offers option to export to doctor

Patient right to privacy should be held to a high standard

- Developers aren’t required to show that their apps are safe and effective unless they’re applying to the FDA for approval. The FDA requires clearance only for apps that act as a medical device or work with a medical device

(https://www.medicaleconomics.com/medical-economics-blog/how-make-health-apps-valuable-physicians-and-patients/page/0/1)

FDA: What counts as a Mobile Medical App?

- Not all mHealth apps are included in this category
- "Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device."

(https://www.fda.gov/medical-devices/digital-health/mobile-medical-applications#a)

Not Just About Security

- "Doctors struggle with which apps to recommend for patients and patients don’t know which apps may be useful. Physicians must consider the value of an mHealth app before they recommend one since most apps have been created without medical expert involvement or appropriate testing validation."

(https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6090170/)

How widespread is this?

- From a 2014 survey, more than a third of physicians had recommended that patients use health apps in the past year.
- (Key findings on physician digital behavior from *Taking the Pulse® U.S. 2014)*

- *This number has no doubt risen, as we see an increase in the usage of mHealth apps.*

primum non nocere

Acknowledgments

- Capsule8
- Summercon Staff
- CU2600

Questions?