JANUARY 27, 2020

eff.org

ELECTRONIC FRONTIER FOUNDATION

# Ring Doorbell App Packed with Third-Party Trackers

ESPAÑOL

Ring isn't just a product that allows users to surveil their neighbors. The company also uses it to surveil its customers.

An investigation by EFF of the Ring doorbell app for Android found it to be packed with third-party trackers sending out a plethora of customers' personally identifiable information (PII). Four main analytics and marketing companies were discovered to be receiving information such as the names, private IP addresses, mobile network carriers, persistent identifiers, and sensor data on the devices of paying customers.

The danger in sending even small bits of information is that analytics and tracking companies are able to combine these bits together to form a unique picture of the user's device. This cohesive whole represents a fingerprint that follows the user as they interact with other apps and use their device, in essence providing trackers the ability to spy on what a user is doing in their digital lives and when they are doing it. All this takes place without meaningful user notification or consent and, in most cases, no way to mitigate the damage done. Even when this information is not misused and employed for precisely its stated purpose (in most cases marketing), this can lead to a whole host of social ills.

Ring has exhibited a pattern of behavior that attempts to mitigate exposure to criticism and scrutiny while benefiting from the wide array of customer data available to them. It has been able to do so by leveraging an image of the secure home, while profiting from a surveillance network which facilitates police departments' unprecedented access into the private lives of citizens, as we have previously covered. For consumers, this image has cultivated a sense of trust in Ring that should be shaken by the reality of how the app functions: not only does Ring mismanage consumer data, but it also intentionally hands over that data to trackers and data miners.

## Findings

Our testing, using Ring for Android version 3.21.1, revealed PII delivery to `branch.io`, `mixpanel.com`, `appsflyer.com` and `facebook.com`. Facebook, via its Graph API, is alerted when the app is opened and upon device actions such as app deactivation after screen lock due to inactivity. Information delivered to Facebook (even if you don't have a Facebook account) includes time zone, device model, language preferences, screen resolution, and a unique identifier (`anon_id`), which persists even when you reset the OS-level advertiser ID.

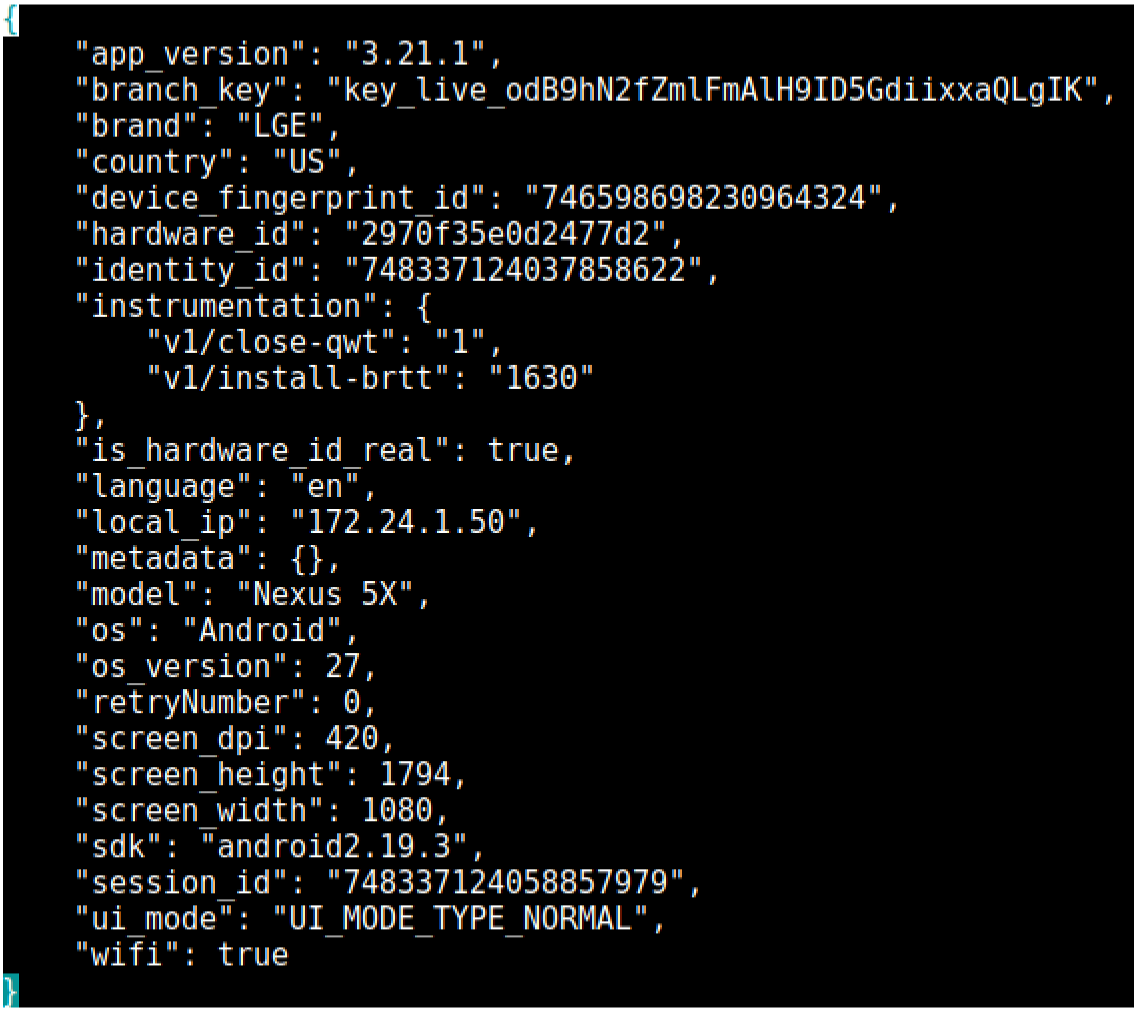
Branch, which describes itself as a "deep linking" platform, receives a number of unique identifiers (`device_fingerprint_id`, `hardware_id`, `identity_id`) as well as your device's local IP address, model, screen resolution, and DPI.

AppsFlyer, a big data company focused on the mobile platform, is given a wide array of information upon app launch as well as certain user actions, such as interacting with the "Neighbors" section of the app. This information includes your mobile carrier, when Ring was installed and first launched, a number of unique identifiers, the app you installed from, and whether AppsFlyer tracking came preinstalled on the device. This last bit of information is presumably to determine whether AppsFlyer tracking was included as bloatware on a low-end Android device. Manufacturers often offset the costs of device production by selling consumer data, a practice that disproportionately affects low-income earners and was the subject of a recent petition to Google initiated by Privacy International and co-signed by EFF.

Most alarmingly, AppsFlyer also receives the sensors installed on your device (on our test device, this included the magnetometer, gyroscope, and accelerometer) and current calibration settings.

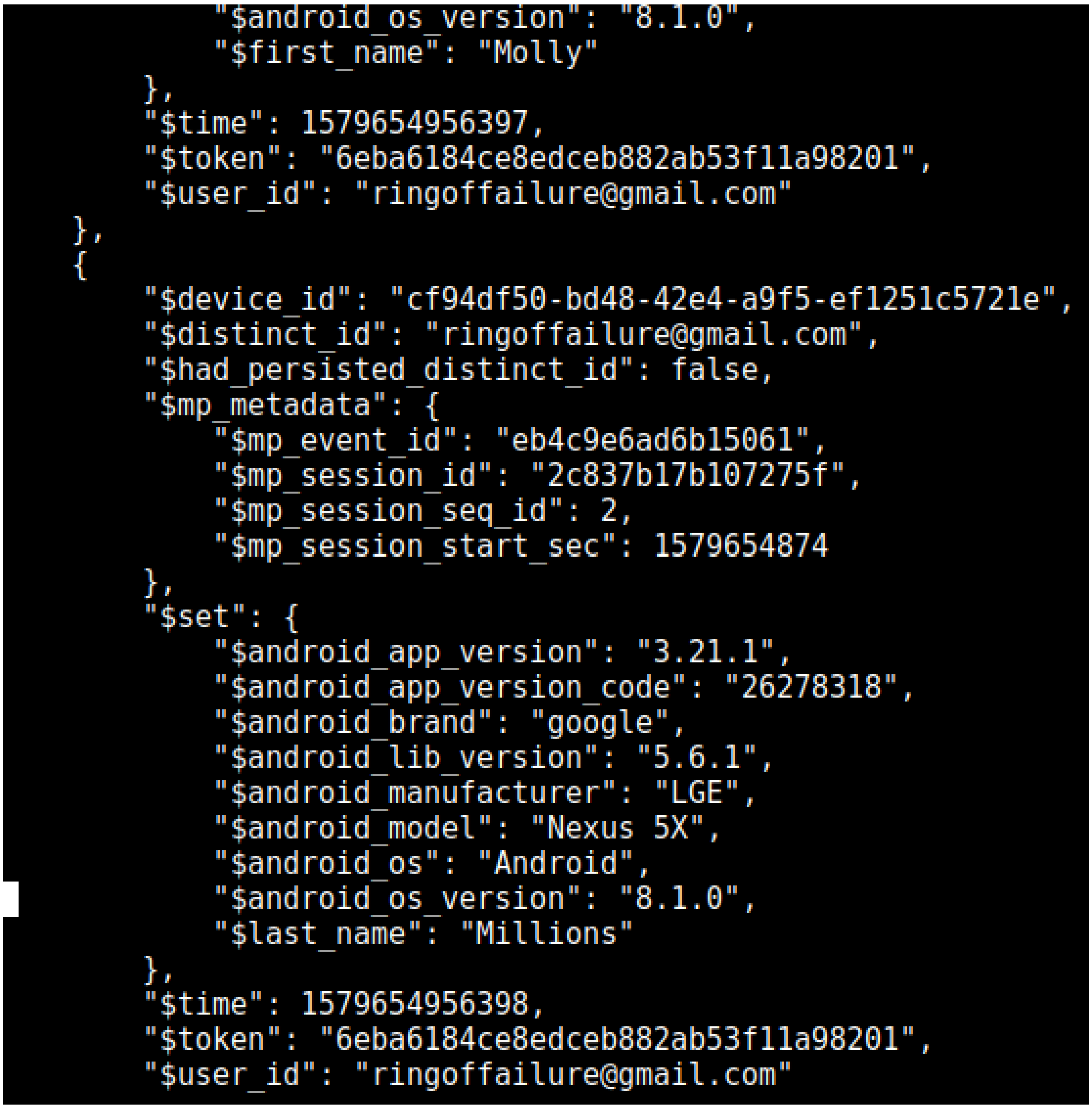
Ring gives MixPanel the most information by far. Users' full names, email addresses, device information such as OS version and model, whether bluetooth is enabled, and app settings such as the number of locations a user has Ring devices installed in, are all collected and reported to MixPanel. MixPanel is briefly mentioned in Ring's list of third party services, but the extent of their data collection is not. None of the other trackers listed in this post are mentioned at all on this page.

Ring also sends information to the Google-owned crash logging service Crashalytics. The exact extent of data sharing with this service is yet to be determined.



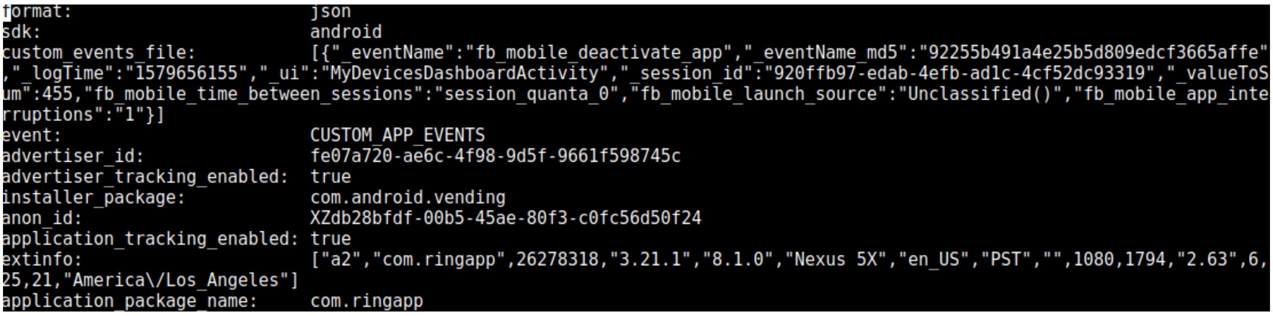
```
{
    "app_version": "3.21.1",
    "branch_key": "key_live_odB9hN2fZmlFmAlH9ID5GdiixxaQLgIK",
    "brand": "LGE",
    "country": "US",
    "device_fingerprint_id": "746598698230964324",
    "hardware_id": "2970f35e0d2477d2",
    "identity_id": "748337124037858622",
    "instrumentation": {
        "v1/close-qwt": "1",
        "v1/install-brtt": "1630"
    },
    "is_hardware_id_real": true,
    "language": "en",
    "local_ip": "172.24.1.50",
    "metadata": {},
    "model": "Nexus 5X",
    "os": "Android",
    "os_version": 27,
    "retryNumber": 0,
    "screen_dpi": 420,
    "screen_height": 1794,
    "screen_width": 1080,
    "sdk": "android2.19.3",
    "session_id": "748337124058857979",
    "ui_mode": "UI_MODE_TYPE_NORMAL",
    "wifi": true
}
```

Data delivered to `api.branch.io`



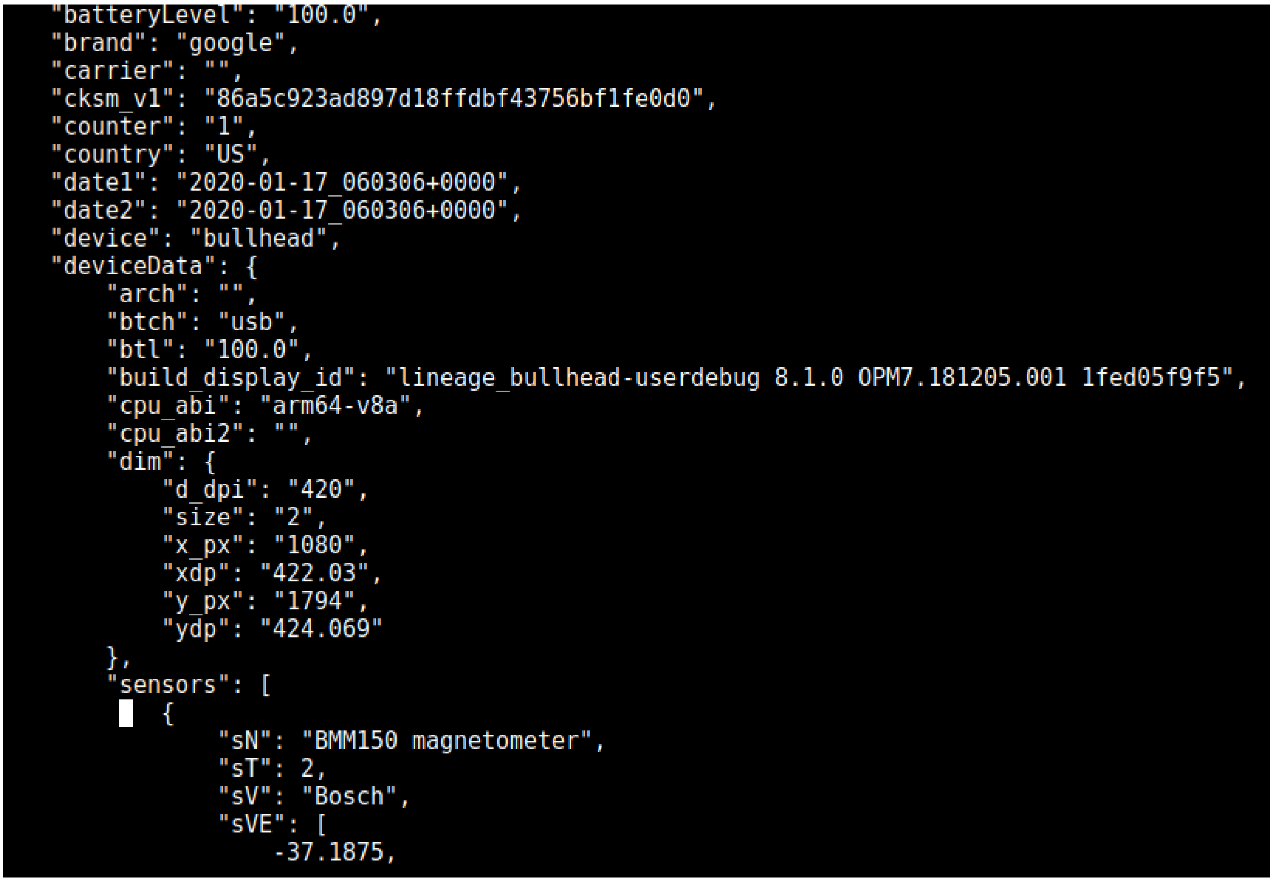
```
            "$android_os_version": "8.1.0",
            "$first_name": "Molly"
        },
        "$time": 1579654956397,
        "$token": "6eba6184ce8edceb882ab53f11a98201",
        "$user_id": "ringoffailure@gmail.com"
    },
    {
        "$device_id": "cf94df50-bd48-42e4-a9f5-ef1251c5721e",
        "$distinct_id": "ringoffailure@gmail.com",
        "$had_persisted_distinct_id": false,
        "$mp_metadata": {
            "$mp_event_id": "eb4c9e6ad6b15061",
            "$mp_session_id": "2c837b17b107275f",
            "$mp_session_seq_id": 2,
            "$mp_session_start_sec": 1579654874
        },
        "$set": {
            "$android_app_version": "3.21.1",
            "$android_app_version_code": "26278318",
            "$android_brand": "google",
            "$android_lib_version": "5.6.1",
            "$android_manufacturer": "LGE",
            "$android_model": "Nexus 5X",
            "$android_os": "Android",
            "$android_os_version": "8.1.0",
            "$last_name": "Millions"
        },
        "$time": 1579654956398,
        "$token": "6eba6184ce8edceb882ab53f11a98201",
        "$user_id": "ringoffailure@gmail.com"
```

Data delivered to `api.mixpanel.com`



```
format:                         json
sdk:                            android
custom_events_file:             [{"_eventName":"fb_mobile_deactivate_app","_eventName_md5":"92255b491a4e25b5d809edcf3665affe"
,"_logTime":"1579656155","_ui":"MyDevicesDashboardActivity","_session_id":"920ffb97-edab-4efb-ad1c-4cf52dc93319","_valueToS
um":455,"fb_mobile_time_between_sessions":"session_quanta_0","fb_mobile_launch_source":"Unclassified()","fb_mobile_app_inte
rruptions":"1"}]
event:                          CUSTOM_APP_EVENTS
advertiser_id:                  fe07a720-ae6c-4f98-9d5f-9661f598745c
advertiser_tracking_enabled:    true
installer_package:              com.android.vending
anon_id:                        XZdb28bfdf-00b5-45ae-80f3-c0fc56d50f24
application_tracking_enabled:   true
extinfo:                        ["a2","com.ringapp",26278318,"3.21.1","8.1.0","Nexus 5X","en_US","PST","",1080,1794,"2.63",6,
25,21,"America\/Los_Angeles"]
application_package_name:       com.ringapp
```

Data delivered to `graph.facebook.com`



```
    "batteryLevel": "100.0",
    "brand": "google",
    "carrier": "",
    "cksm_v1": "86a5c923ad897d18ffdbf43756bf1fe0d0",
    "counter": "1",
    "country": "US",
    "date1": "2020-01-17_060306+0000",
    "date2": "2020-01-17_060306+0000",
    "device": "bullhead",
    "deviceData": {
        "arch": "",
        "btch": "usb",
        "btl": "100.0",
        "build_display_id": "lineage_bullhead-userdebug 8.1.0 OPM7.181205.001 1fed05f9f5",
        "cpu_abi": "arm64-v8a",
        "cpu_abi2": "",
        "dim": {
            "d_dpi": "420",
            "size": "2",
            "x_px": "1080",
            "xdp": "422.03",
            "y_px": "1794",
            "ydp": "424.069"
        },
        "sensors": [
            {
                "sN": "BMM150 magnetometer",
                "sT": 2,
                "sV": "Bosch",
                "sVE": [
                    -37.1875,
```

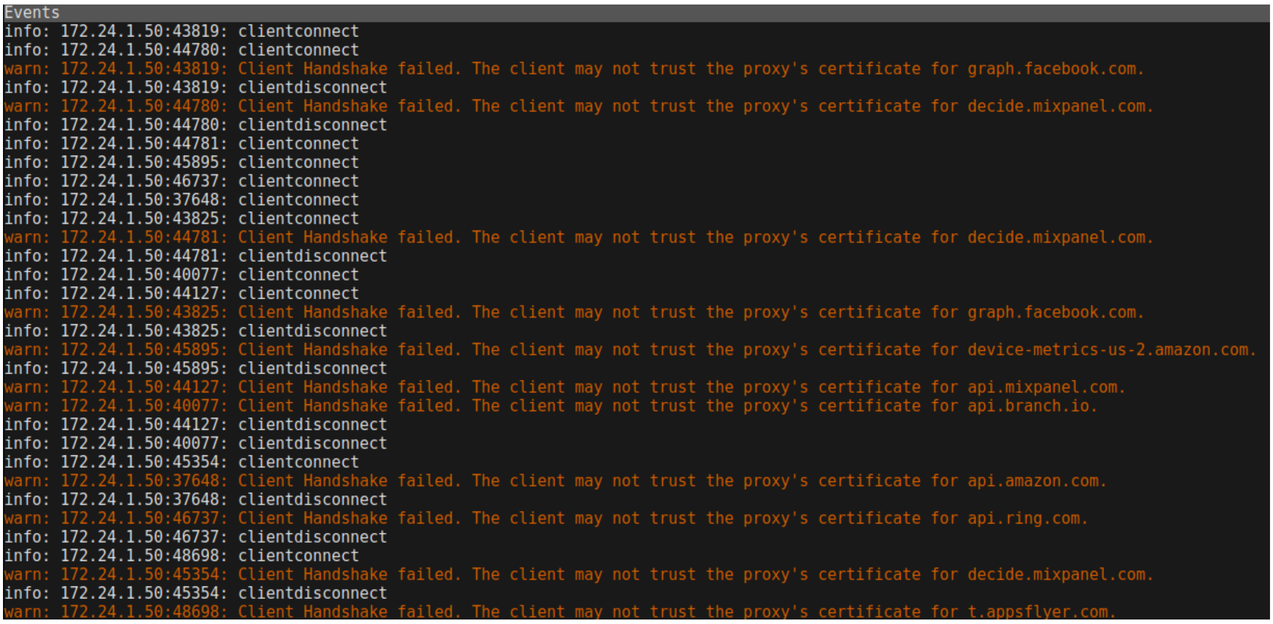
Data delivered to `t.appsflyer.com`

## Methodology

All traffic we observed on the app was being sent using encrypted HTTPS. What's more, the encrypted information was delivered in a way that eludes analysis, making it more difficult (but not impossible) for security researchers to learn of and report these serious privacy breaches.

Our dynamic analysis was performed using `mitmproxy` running on an access point to intercept and analyze HTTPS flows from an Android test device. To remove noise generated from other apps, we installed the AFWall+ firewall app and only allowed network traffic from Ring. `mitmproxy` generates a root x509 certificate which is to be installed in the OS-level certificate store in Android, allowing active interception to take place on otherwise secured traffic. This led us to the initial discovery that the root certificate was not being accepted as valid, and that some form of certificate pinning was being employed by the app.

App-level certificate pinning is when an app validates the certificates of a remote server against a record of that certificate stored within the app, rather than validating against the list of root certificates within the OS. This is often used as a security measure, to ensure that misissuance of certificates or mismanagement along the chain of trust in PKI does not compromise the integrity, confidentiality, or authenticity of HTTPS traffic. Unfortunately, it can also prevent security researchers and users from seeing exactly what information these devices are sending, and to whom. In the case of Ring, we initially observed all intercepted traffic upon launch being rejected, and were not able to observe any communications.



```
Events
info: 172.24.1.50:43819: clientconnect
info: 172.24.1.50:44780: clientconnect
warn: 172.24.1.50:43819: Client Handshake failed. The client may not trust the proxy's certificate for graph.facebook.com.
info: 172.24.1.50:43819: clientdisconnect
warn: 172.24.1.50:44780: Client Handshake failed. The client may not trust the proxy's certificate for decide.mixpanel.com.
info: 172.24.1.50:44780: clientdisconnect
info: 172.24.1.50:44781: clientconnect
info: 172.24.1.50:45895: clientconnect
info: 172.24.1.50:46737: clientconnect
info: 172.24.1.50:37648: clientconnect
info: 172.24.1.50:43825: clientconnect
warn: 172.24.1.50:44781: Client Handshake failed. The client may not trust the proxy's certificate for decide.mixpanel.com.
info: 172.24.1.50:44781: clientdisconnect
info: 172.24.1.50:40077: clientconnect
info: 172.24.1.50:44127: clientconnect
warn: 172.24.1.50:43825: Client Handshake failed. The client may not trust the proxy's certificate for graph.facebook.com.
info: 172.24.1.50:43825: clientdisconnect
warn: 172.24.1.50:45895: Client Handshake failed. The client may not trust the proxy's certificate for device-metrics-us-2.amazon.com.
info: 172.24.1.50:45895: clientdisconnect
warn: 172.24.1.50:44127: Client Handshake failed. The client may not trust the proxy's certificate for api.mixpanel.com.
warn: 172.24.1.50:40077: Client Handshake failed. The client may not trust the proxy's certificate for api.branch.io.
info: 172.24.1.50:44127: clientdisconnect
info: 172.24.1.50:40077: clientdisconnect
info: 172.24.1.50:45354: clientconnect
warn: 172.24.1.50:37648: Client Handshake failed. The client may not trust the proxy's certificate for api.amazon.com.
info: 172.24.1.50:37648: clientdisconnect
warn: 172.24.1.50:46737: Client Handshake failed. The client may not trust the proxy's certificate for api.ring.com.
info: 172.24.1.50:46737: clientdisconnect
info: 172.24.1.50:48698: clientconnect
warn: 172.24.1.50:45354: Client Handshake failed. The client may not trust the proxy's certificate for decide.mixpanel.com.
info: 172.24.1.50:45354: clientdisconnect
warn: 172.24.1.50:48698: Client Handshake failed. The client may not trust the proxy's certificate for t.appsflyer.com.
```

`mitmproxy` screen displaying results of certificate pinning

It was only through the powerful dynamic analysis framework Frida that we were able to inject code into Ring at runtime, which ensured that the certificate provided by our `mitmproxy` instance would be accepted as valid. This allowed us to inspect all HTTPS traffic sent through the app.

## Conclusion

Ring claims to prioritize the security and privacy of its customers, yet time and again we've seen these claims not only fall short, but harm the customers and community members who engage with Ring's surveillance system. In the past, we've illuminated the mismanagement of user information which has led to data breaches, and the attempt to place the blame for such blunders at the customers' feet.

This goes a step beyond that, by simply delivering sensitive data to third parties not accountable to Ring or bound by the trust placed in the customer-vendor relationship. As we've mentioned, this includes information about your device and carrier, unique identifiers that allow these companies to track you across apps, real-time interaction data with the app, and information about your home network. In the case of MixPanel, it even includes your name and email address. This data is given to parties either only mentioned briefly, buried on an internal page users are unlikely to ever see, or not listed at all.

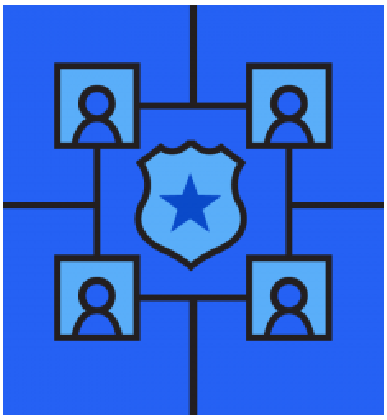
`mitmproxy` flow files:

- mitmproxy-1.flows__.txt
- mitmproxy-2.flows__.txt

# RELATED UPDATES

DEEPLINKS BLOG BY SARAH HAMID | FEBRUARY 6, 2025

### EFF Applauds Little Rock, AR for Cancelling ShotSpotter Contract



DEEPLINKS BLOG BY BERYL LIPTON, DAVE MAASS | JANUARY 28, 2025

### California Law Enforcement Misused State Databases More Than 7,000 Times in 2023

DEEPLINKS BLOG BY MATTHEW GUARIGLIA | JANUARY 15, 2025

### Police Use of Face Recognition Continues to Wrack Up Real-World Harms

DEEPLINKS BLOG BY MATTHEW GUARIGLIA | DECEMBER 31, 2024

### AI and Policing: 2024 in Review

### Aerial and Drone Surveillance: 2024 in Review

DEEPLINKS BLOG BY HANNAH ZHAO | DECEMBER 29, 2024

DEEPLINKS BLOG BY MATTHEW GUARIGLIA | DECEMBER 25, 2024

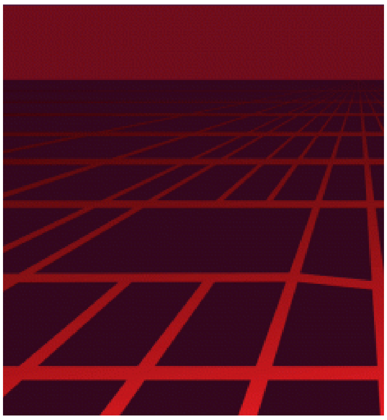
## Police Surveillance in San Francisco: 2024 in Review

DEEPLINKS BLOG BY BERYL LIPTON, DAVE MAASS | DECEMBER 24, 2024

## The Atlas of Surveillance Expands Its Data on Police Surveillance Technology: 2024 in Review

## FTC Rightfully Acts Against So-Called “AI Weapon Detection” Company Evolv

DEEPLINKS BLOG BY MATTHEW GUARIGLIA, COOPER QUINTIN | DECEMBER 6, 2024



DEEPLINKS BLOG BY BILL BUDINGTON | NOVEMBER 8, 2024

## Creators of This Police Location Tracking Tool Aren't Vetting Buyers. Here's How To Protect Yourself

DEEPLINKS BLOG BY BERYL LIPTON | NOVEMBER 5, 2024

## AI in Criminal Justice Is the Trend Attorneys Need to Know About

ELECTRONIC FRONTIER FOUNDATION
eff.org