Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Προστασία Προσωπικών Δεδομένων στις «έξυπνες» Εφαρμογές Παρακολούθησης Φυσικής Κατάστασης

Κυριάκος Μάγος

Επιβλέπων Καθηγητής

Δρ. Κωνσταντίνος Λιμνιώτης

Δεκέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Προστασία Προσωπικών Δεδομένων στις «έξυπνες» Εφαρμογές Παρακολούθησης Φυσικής Κατάστασης

Κυριάκος Μάγος

Επιβλέπων Καθηγητής

Δρ. Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2019

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Ο σκοπός της μεταπτυχιακής διατριβής είναι η διερεύνηση διαφόρων δημοφιλών εφαρμογών παρακολούθησης φυσικής κατάστασης, προκειμένου να εξεταστεί κατά πόσο γίνεται επεξεργασία προσωπικών δεδομένων χωρίς την γνώση και συγκατάθεση του χρήστη. Στο πλαίσιο αυτό εξετάζεται επίσης και εάν υπάρχουν διαρροές αυτών των δεδομένων σε διάφορες βιβλιοθήκες τρίτων μελών για διαφημιστικούς σκοπούς και, σε καταφατική περίπτωση, εξετάζεται αν γίνεται ανώνυμα. Η σπουδαιότητα των ερωτημάτων αυτών έγκειται στις απαιτήσεις για νόμιμη επεξεργασία προσωπικών δεδομένων που τίθενται με το ισχύον νομικό πλαίσιο στην Ευρωπαϊκή Ένωση (ιδίως με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων), σε συνδυασμό με το γεγονός ότι οι εν λόγω εφαρμογές μπορούν να επεξεργαστούν και ευαίσθητες πληροφορίες υγείας των χρηστών. Απώτερος στόχος είναι να αξιολογηθούν αυτά τα δεδομένα κατά πόσο θα μπορούσαν να οδηγήσουν στην εξαγωγή συμπερασμάτων για την φυσική κατάσταση του χρήστη.

Αρχικώς, αφού παρατίθενται μερικοί προβληματισμοί ως προς την εξέλιξη αυτής της κατηγορίας συσκευών και εφαρμογών σε σχέση με την ιδιωτικότητα των χρηστών, στη συνέχεια αναλύονται οι πολιτικές απορρήτου της κάθε επιλεγμένης εφαρμογής φυσικής κατάστασης.

Για την αξιολόγηση των παραπάνω σχεδιάστηκε πειραματική διάταξη όπου εξετάζονται οι επιλεχθείσες εφαρμογές φυσικής κατάστασης μέσω ενός περιβάλλοντος «Man-In-The Middle» από εξειδικευμένη εφαρμογή και αξιολογούνται όλα τα δεδομένα που εξέρχονται από τις εφαρμογές αυτές.

Από τα αποτελέσματα της έρευνας προκύπτει ότι υπάρχει όντως αρκετά μεγάλη συλλογή δεδομένων προσωπικού χαρακτήρα από όλες τις εφαρμογές, οι οποίες συλλέγουν αυτά που αναφέρουν στις αναφορές ιδιωτικότητας τους (αν και κάποιες εξ αυτών δεν παρέχουν απόλυτα σαφή ενημέρωση). Παράλληλα η μεγάλη ποικιλία αυτών των δεδομένων κάνει δυνατή την εξαγωγή συμπερασμάτων για τον χρήστη, όπως και την δημιουργία του προφίλ αυτού.

Summary

The purpose of this thesis is to investigate various popular fitness monitoring applications, towards examining whether personal data are being processed without the user's knowledge and consent. In this framework, possible data leakages to various third-party libraries for, e.g., advertising purposes, are also investigated, and, if this is indeed the case, the anonymity of these data is being studied. The significance of these issues rests with the increased legal obligations for personal data protection stemming from the European legal framework (especially from the General Data Protection Regulation), in conjunction with the fact that such applications may process sensitive health data. The ultimate goal is to evaluate the whole process with respect to whether such applications lead to the derivation of conclusions about the user's physical condition.

First, a discussion is presented regarding some concerns about the evolution of this category of devices and applications with respect to users privacy. Next, the privacy policies of such applications are being studied and analysed.

To evaluate the underlying personal data processing, a testing environment has been created to perform appropriate experiments on selected fitness applications through a Man-in-The-Middle set-up. A specialized software tool is being utilized to capture and evaluate all outgoing data in runtime.

The results exhibit that a fairly large amount of personal data from all applications was collected; although the corresponding privacy policies describe such processes, it is questionable whether the information provided is clear. Moreover, the amount of data collected may yield to drawing conclusions for the user as well as to create his profile.

Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή έγινε στο πλαίσιο του Μεταπτυχιακού Προγράμματος «Ασφάλεια Υπολογιστών και Δικτύων» της Σχολής Θετικών και Εφαρμοσμένων Επιστημών.

Πριν την παρουσίαση των αποτελεσμάτων δεν θα μπορούσα παρά να ευχαριστήσω ορισμένους από τους ανθρώπους που διαδραμάτισαν πολύ σημαντικό ρόλο στην ολοκλήρωση της μεταπτυχιακής διατριβής.

Πρώτο από όλους θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή της μεταπτυχιακής διατριβής Καθηγητή κ. Λιμνιώτη Κωνσταντίνο, για την πολύτιμη βοήθεια και καθοδήγηση αλλά και την εκτίμηση που έδειξε στο πρόσωπό μου.

Παράλληλα θα ήθελα να ευχαριστήσω την αρραβωνιαστικιά μου Μιχαέλλα Ραφαέλλα Θωμά για την αμέριστη κατανόηση που μου έδειξε αλλά και το κουράγιο και την απαραίτητη ηθική συμπαράσταση προς την ολοκλήρωση της μεταπτυχιακής διατριβής.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Σκοπός της έρευνας

Μια σημαντική κατηγορία «έξυπνων» εφαρμογών, που είναι αρκετά δημοφιλείς, είναι οι εφαρμογές παρακολούθησης φυσικής κατάστασης. Αυτές οι εφαρμογές βοηθούν τον χρήστη παρουσιάζοντάς του στατιστικά από την δραστηριότητά του, όπως τα χιλιόμετρα που διένυσε, τις θερμίδες που κατανάλωσε κτλ.

Ωστόσο, όπως και σε κάθε «έξυπνη» εφαρμογή προκύπτουν σημαντικά ζητήματα ως προς την προστασία των προσωπικών δεδομένων των χρηστών. Ένα παράδειγμα είναι η υπέρμετρη συλλογή προσωπικών δεδομένων των χρηστών (περισσότερα δηλαδή από αυτά που χρειάζονται για την επεξεργασία των δεδομένων) και η ενδεχόμενη αποστολή τους σε τρίτα μέλη χωρίς την πλήρης ενημέρωση του χρήστη. Οι πιο πάνω προβληματισμοί αποκτούν ακόμα μεγαλύτερη σημασία στις εφαρμογές παρακολούθησης φυσικής κατάστασης διότι τα δεδομένα που συλλέγονται ενδεχομένως να αποκαλύπτουν και πληροφορίες υγείας, γεγονός που τα καθιστά ευαίσθητα – οπότε οι συνέπειες αποκάλυψής τους σε τρίτους μπορούν να είναι εξαιρετικά δυσμενείς.

Στην παρούσα μεταπτυχιακή διατριβή θα μελετηθούν δημοφιλείς εφαρμογές παρακολούθησης φυσικής κατάστασης ως προς τα δεδομένα που συλλέγουν ή/και αποστέλλουν σε τρίτα μέλη, με απώτερο στόχο να διερευνηθεί αφενός αν γίνεται επεξεργασία δεδομένων χωρίς την γνώση και συγκατάθεση του χρήστη και αφετέρου αν τρίτα μέλη (π.χ. διαφημιστικά δίκτυα) συλλέγουν υπέρμετρη πληροφορία που δύναται να οδηγήσει σε εξαγωγή συμπερασμάτων για τη φυσική κατάσταση ή/και την υγεία του χρήστη. Στο πλαίσιο αυτό θα πραγματοποιηθεί δυναμική ανάλυση στις επιλεχθείσες εφαρμογές με κατάλληλα εργαλεία λογισμικού, προκειμένου να «ανιχνευτούν» σε

πραγματικό χρόνο οι ροές δεδομένων από τη συσκευή του χρήστη. Θα μελετηθεί επίσης ποιες είναι οι πιο συχνές βιβλιοθήκες τρίτων μελών (third party libraries) τις οποίες χρησιμοποιούν οι εφαρμογές αυτές, προκειμένου να διερευνηθεί σε ποιες άλλες συνηθισμένες εφαρμογές χρησιμοποιούνται οι βιβλιοθήκες αυτές – και τούτο διότι η χρήση της ίδιας βιβλιοθήκης από διαφορετικές εφαρμογές, ενδεχομένως με διαφορετικά δικαιώματα, μπορεί να εγείρει σημαντικά ζητήματα ως προς την ιδιωτικότητα του χρήστη (δημιουργία υπέρμετρου προφίλ χρήστη, ενδεχομένως και ευαίσθητων δεδομένων).

1.2 Βασικά Ερευνητικά Ερωτήματα

Η έρευνα αυτή μελετάει κυρίως τη σχέση μεταξύ της διαδικασίας συλλογής πληροφοριών και των τρόπων μετάδοσής τους στις εφαρμογές παρακολούθησης της φυσικής κατάστασης αλλά και των συσκευών που μπορούν να φορεθούν (wearable) των εφαρμογών αυτών, τις υπηρεσίες cloud που αποθηκεύουν τα δεδομένα τους και εάν third parties έχουν πρόσβαση σε αυτά τα προσωπικά δεδομένα από αυτές τις συσκευές. Από αυτό εξάγονται τα ακόλουθα ερευνητικά ερωτήματα:

- Τα δεδομένα που συλλέγονται είναι αυτά που αναφέρει η πολιτική ιδιωτικότητας (privacy policy) της εφαρμογής;
- Οι εφαρμογές αυτές συλλέγουν μόνο όσα δεδομένα χρειάζονται για την επεξεργασία δεδομένων;
- Οι εφαρμογές αυτές αποστέλλουν πληροφορίες σε τρίτα μέλη και εάν γίνεται αυτό, ο χρήστης ενημερώνεται και έχει το δικαίωμα να αρνηθεί;
- Τα δεδομένα που συλλέγονται είναι δυνατόν να οδηγήσουν σε συμπεράσματα για την υγεία του χρήστη;
- Είναι πιθανό ένα τρίτο μέλος να συλλέξει δεδομένα από διάφορες εφαρμογές με σκοπό να δημιουργήσει προφίλ για τα υποκείμενα των δεδομένων;

Τα ανωτέρω ερωτήματα θα εξεταστούν και υπό το πρίσμα του σχετικού νομικού πλαισίου για την προστασία προσωπικών δεδομένων. Απαντώντας στα ερωτήματα αυτά για την κάθε περίπτωση θα είναι ξεκάθαρο ποιες εφαρμογές και εταιρίες προσφέρουν εφαρμογές και υπηρεσίες περισσότερο φιλικές προς την ιδιωτικότητα.

1.3 Δομή της μεταπτυχιακής διατριβής

Η διατριβή αποτελείται από εφτά κεφάλαια. Σε αυτά τα κεφάλαια θα αναλυθούν και θα ερευνηθούν τα παρακάτω:

Αρχικά στο δεύτερο κεφάλαιο της μεταπτυχιακής διατριβής περιγράφονται βασικές έννοιες αλλά και ορισμοί σε σχέση με την νομοθεσία και γίνεται μία σύντομη ιστορική αναδρομή στο κομμάτι της ιδιωτικότας από τον καιρό της Αρχαίας Ελλάδας μέχρι σήμερα. Ακολούθως περιγράφονται τα κυριότερα άρθρα του Γενικού Κανονισμού Προστασίας Δεδομένων.

Στην συνέχεια στο τρίτο κεφάλαιο αναλύονται οι θέματα ιδιωτικότητας και προστασίας δεδομένων που προκύπτουν από την χρήση έξυπνων συσκευών και εφαρμογών, όπου με αυτά θα γίνεται αντιληπτός ο σκοπός της μεταπτυχιακής διατριβής.

Στο τέταρτο κεφάλαιο εξηγείται τι είναι η εφαρμογή παρακολούθησης φυσικής κατάστασης ενώ παράλληλα επιλέγονται οι εφαρμογές που θα αξιολογηθούν ενώ παράλληλα γίνεται έρευνα στις πολιτικές απορρήτου της κάθε εφαρμογής.

Ακολούθως στο πέμπτο κεφάλαιο εξηγείται ο τρόπος με τον οποίο θα αξιολογηθούν οι επιλεγμένες εφαρμογές παρακολούθησης φυσικής κατάστασης, τι εφαρμογές θα χρησιμοποιηθούν για την αξιολόγηση και τέλος παρουσιάζονται τα αποτελέσματα της έρευνας.

Στο έκτο κεφάλαιο θα αναλυθούν και θα σχολιαστούν τα αποτελέσματα του πέμπτου κεφαλαίου ως προς τα ερευνητικά ερωτήματα που τέθηκαν στο παρόν κεφάλαιο.

Τέλος στο έβδομο κεφάλαιο γίνεται μία σύνοψη της διατριβής, περιγράφονται οι περιορισμοί της έρευνας και γίνεται αναφορά σε πιθανή σχετική μελλοντική έρευνα.

Κεφάλαιο 2

Προστασία προσωπικών δεδομένων – Θεσμικό Πλαίσιο

2.1 Γενικά

Σε αυτό το κεφάλαιο θα περιγραφούν βασικές έννοιες και ορισμοί σε σχέση με τη νομοθεσία για την προστασία προσωπικών δεδομένων.

2.2 Τι είναι προσωπικά δεδομένα

Τα προσωπικά δεδομένα ή δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. (European Commision 2018) Πιο συγκεκριμένα ο Ευρωπαϊκός Γενικός Κανονισμός Προστασίας Δεδομένων (European Parliament, Council of the European Union 2016), ο οποίος είναι σε εφαρμογή όλα τα Κράτη-Μέλη της Ευρωπαϊκής Ένωσης από τις 25 Μαΐου 2018, αναφέρει ότι είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. Με άλλα λόγια είναι οτιδήποτε μπορεί να χαρακτηρίσει ή να ξεχωρίσει ένα άτομο από ένα άλλο.

Η ανάγκη για προστασία των προσωπικών δεδομένων, η οποία είναι συνυφασμένη – αν και δεν ταυτίζεται - με την έννοια της ιδιωτικότητας - έχει αρκετά βαθιά τις ρίζες της στην ιστορία. Η πρώτη επίσημη ανάγκη για διάκριση του δημόσιου βίου μεταξύ του ιδιωτικού καταγράφεται από τον Αριστοτέλη[1]. Αιώνες αργότερα στην Γαλλική Επανάσταση κατά την οποία ο Saint Just διακήρυττε ότι η ελευθερία των ανθρώπων βρίσκεται στην ιδιωτική τους ζωή και ότι θα πρέπει να προστατεύεται η ιδιωτική ζωή του κάθε ανθρώπου[2] πράγμα που για τον καιρό θα μπορούσε να χαρακτηριστεί το λιγότερο ριζοσπαστικό.

Αργότερα ξεκινά να εμφανίζεται η έννοια της προστασίας της ιδιωτικότητας στις ΗΠΑ με το άρθρο αναθεώρησης νομοθεσίας των Warren και Brandeis (S. D. Warren and Brandeis 1890) στο Harvard Law Review το οποίο για πρώτη φορά το 1890 αναλύει και χαρακτηρίζει την ιδωτικότητα ως το δικαίωμα του κάθε ατόμου «να τον αφήσουν ήσυχο». Είναι το πρώτο άρθρο στο οποίο περιγράφει ότι θα έπρεπε να εξετάζεται στο δικαστήριο το δικαίωμα της ιδιωτικότητας όπως για πρώτη φορά την περιγράφει. Μετά από αυτό ακολούθησαν αρκετά άλλα άρθρα και νόμοι οι οποίοι εμπλούτιζαν κατά καιρούς αυτό το δικαίωμα.

Στην Ευρώπη οι πρώτες νομοθεσίες για την προστασία των προσωπικών δεδομένων εμφανίστηκαν την δεκαετία του ‘70 και συγκεκριμένα στην Γερμανία, Αυστρία, Γαλλία και σκανδιναβικές χώρες όταν ξεκίνησε η επεξεργασία δεδομένων των πολιτών της κάθε χώρας σε μεγάλη κλίμακα. Η ανάγκη αυτή αυξήθηκε κατά την δεκαετία του ’80 όταν ιδιωτικές εταιρίες ξεκίνησαν να μαζεύουν προσωπικά δεδομένα των πελατών τους. Αυτό άλλαξε με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ (Data Protection Directive) (European Parliament, Council of the European Union 1995) το 1995, στην οποία μπαίνουν γερά θεμέλια στην προστασία των δεδομένων προσωπικού χαρακτήρα από την επεξεργασία και την ελεύθερη διακίνηση των δεδομένων. Αυτή η οδηγία οδήγησε τα κράτη μέλη σε αλλαγές στην νομοθεσία για να εναρμονιστούν με αυτή. Αυτό φυσικά είχε επίδραση διεθνώς σε αυτό τον τομέα.

Όσον αφορά τον τομέα των τηλεπικοινωνιών και του διαδικτύου υπήρχε ανάγκη για λήψη μέτρων για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η Ε.Ε. στην προσπάθεια της να προστατέψει τους πολίτες της ψήφισε αρχικά την οδηγία 97/66/ΕΚ (Telecommunications Data Protection Directive) (European Parliament, Council of the

[1] «…απόσταση, χώρος και απομόνωση από τη δημόσια ζωή…», Αριστοτέλης «Ηθικά Νικομάχεια»
[2] Saint Just «Fragments sur les institutions républicaines»

European Union 1998) η οποία θεωρήθηκε αναγκαία για την προστασία των δικαιωμάτων και ελευθεριών των Ευρωπαίων στον ειδικότερο τομέα των τηλεπικοινωνιών. Ωστόσο η ραγδαία εξέλιξη της τεχνολογίας, έκανε τις εκάστοτε οδηγίες παρωχημένες σε διαστήματα μόλις μερικών ετών. Στην προσπάθεια της η Ε.Ε. για εναρμονισμό και προστασία των πολιτών της τροποποιεί την οδηγία 97/66/ΕΚ αρχικά με την νέα οδηγία 2002/58/ΕΚ (European Parliament, Council of the European Union 2002) όπου μετονομάζεται σε «ePrivacy Directive», η οποία τροποποιήθηκε σε ορισμένα σημεία με τις μετέπειτα 2006/24/ΕΚ και 2009/136/ΕΚ (European Parliament, Council of the European Union 2009). Η Οδηγία 2002/58/ΕΚ (ePrivacy Directive) βρίσκεται σε ισχύ και είναι ένα πιο ειδικευμένο νομικό πλαίσιο κυρίως για τους πάροχους διαδικτύου και τηλεφωνίας όπως και για τις επικοινωνίες σε γενικότερο πλαίσιο το οποίο λειτουργεί παράλληλα με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Ρυθμίζει ωστόσο θέματα εγκατάστασης αρχείων σε τερματικές συσκευές χρηστών (όπως, π.χ., είναι η περίπτωση εγκατάστασης των λεγόμενων cookies) ή και πρόσβασης σε πληροφορίες που υπάρχουν σε μία συσκευή, θέτοντας - κατ' αναλογία με τον ΓΚΠΔ - ειδικούς κανόνες για λήψη συγκατάθεσης".

2.3 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Η Ευρωπαϊκή Ένωση (ΕΕ) το 2016 προχώρησε στην εκπόνηση του Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation – εφεξής, Κανονισμός ή GDPR) (European Parliament, Council of the European Union 2016) που αποτελεί Ευρωπαϊκό Κανονισμό, με σκοπό την κατάργηση των υφιστάμενων νομοθεσιών των χωρών κρατών μελών και την εναρμόνιση τους με ένα ενιαίο κανονισμό – νόμο σε όλη την ΕΕ. Έρχεται να αντικαταστήσει την (European Parliament, Council of the European Union 1995) και έχει τεθεί σε εφαρμογή, όπως προαναφέρθηκε, από τις 25 Μαΐου 2018. Η θέσπιση του Κανονισμού ήταν επιβεβλημένη διότι μέσα στην 20ετία υπήρξαν τεράστιες τεχνολογικές εξελίξεις οι οποίες έφεραν νέες προκλήσεις στην προστασία των δεδομένων προσωπικού χαρακτήρα, όπως τα μέσα κοινωνικής δικτύωσης, cloud computing, τεχνολογίες big data κ.α.

Μία από τις πιο μεγάλες αλλαγές που επιφέρει ο νέος Κανονισμός είναι ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα των πολιτών της ΕΕ προστατεύεται ανεξάρτητα εάν η επεξεργασία αυτών των δεδομένων γίνεται από χώρα εκτός ΕΕ. Φυσικά, όπως εξηγεί ο

Bhaskar Chakravorti στο (B. Chakravorti 2018) ο Κανονισμός αυτός όχι μόνο έχει επηρεάσει, αλλά έχει γίνει μοντέλο και για εταιρείες εκτός ΕΕ αφού αυτές εξυπηρετούν πελάτες από χώρες της ΕΕ άρα οι κυρώσεις από το GDPR εμπίπτουν σε αυτές. Ένα παράδειγμα που αναφέρει είναι αυτό του Facebook, όπου το 2017 ανακοίνωσε έσοδα $12.7 δις και λόγω των παραβάσεων της ιδιωτικότητας των χρηστών του κινδυνεύει με πρόστιμο που φτάνει το 4% των παγκόσμιων εσόδων του.

2.3.1 Έννοιες – Ορισμοί

Ο Κανονισμός είναι ένα μεγάλο κείμενο, με πλήθος εννοιών προκειμένου να καλύπτονται όλες οι πιθανές πτυχές μία επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Στην παρούσα ενότητα θα παραθέσουμε απλά κάποιες βασικές έννοιες που υπάρχουν στον Κανονισμό, οι οποίες είναι απαραίτητο να περιγραφούν εν όψει της παρούσας μεταπτυχιακής διατριβής.

Επεξεργασία Δεδομένων: Κάθε εργασία που κάνει ένα φυσικό ή νομικό πρόσωπο ή υπηρεσία ή δημοσία αρχή όπως συλλογή, καταχώριση, οργάνωση, αποθήκευση, τροποποίηση, εξαγωγή, ανάκτηση, αναζήτηση, χρήση, ανακοίνωση, διαβίβαση, διασύνδεση, δέσμευση, διαγραφή και καταστροφή.

Υποκείμενο δεδομένων (data subject): το φυσικό πρόσωπο στο οποίο αφορούν τα δεδομένα.

Υπεύθυνος επεξεργασίας (data controller): το (φυσικό ή νομικό) πρόσωπο που καθορίζει το σκοπό και τον τρόπο επεξεργασίας.

Εκτελών την επεξεργασία (data processor): το (φυσικό ή νομικό) πρόσωπο που δρα για λογαριασμό του υπεύθυνου επεξεργασίας.

Ευαίσθητα προσωπικά δεδομένα: Στην ενότητα 1.2 έγινε αναφορά τι είναι προσωπικά δεδομένα. Στην οδηγία (European Parliament, Council of the European Union 1995) ορίζονται κάποια δεδομένα ως ευαίσθητα (δεδομένα ειδικών κατηγοριών), λόγω του ότι αυτά τα δεδομένα χρήζουν μεγαλύτερης προστασίας διότι εμπίπτουν στον πυρήνα της ιδιωτικότητας του κάθε ατόμου. Αυτά τα δεδομένα είναι:

- φυλετική ή εθνική προέλευση,
- πολιτικά φρονήματα,
- θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
- συμμετοχή σε συνδικαλιστική οργάνωση,
- υγεία,
- κοινωνική πρόνοια,
- ερωτική ζωή,
- ποινικές διώξεις ή καταδίκες,
- στη συμμετοχή σε συναφείς με τα παραπάνω ενώσεις

Ο Κανονισμός (European Parliament, Council of the European Union 2016) στο άρθρο 9 ορίζει επίσης τα δεδομένα ειδικών κατηγοριών, όπως και η προηγούμενη Οδηγία, προσθέτοντας όμως σε αυτά δύο νέες κατηγορίες: τα γενετικά δεδομένα, όπως προκύπτουν από αναλύσεις DNA ή RNA και τα βιομετρικά δεδομένα εφόσον επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου, δακτυλοσκοπικά δεδομένα, εικόνες ίριδας κ.α. Αξίζει ωστόσο να σημειωθεί ότι τα δεδομένα κοινωνικής πρόνοιας (π.χ. πληροφορίες αν κάποιος λαμβάνει επίδομα ανεργίας) δεν χαρακτηρίζονται πλέον, με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ως ευαίσθητα δεδομένα.

Ανώνυμα δεδομένα: είναι τα δεδομένα στα οποία δεν μπορεί να διαπιστωθεί η ταυτότητα ενός προσώπου ακόμα και αν χρησιμοποιηθούν το σύνολο των μέσων που ευλόγως υπάρχουν ή και μπορούν να αξιοποιηθούν με σκοπό την αποκάλυψη της ταυτότητας του προσώπου. Με άλλα λόγια πρέπει να είναι πρακτικά απολύτως αδύνατο να ταυτοποιηθεί κάποιος και όχι απλά να υπάρχει μια πολύ μικρή πιθανότητα (γεγονός που καθιστά τον ασφαλή χαρακτηρισμό δεδομένων ως ανώνυμα μία όχι εύκολη διαδικασία). Πάνω σε αυτά τα ανώνυμα δεδομένα ο κανονισμός (European Parliament, Council of the European Union 2016) αναφέρεται ρητώς πως δεν εφαρμόζεται αφού τα ανώνυμα δεδομένα δεν αποτελούν προσωπικά δεδομένα.

Ψευδωνυμοποιημένα δεδομένα: Είναι τα δεδομένα τα οποία αφού έχουν τύχει επεξεργασίας δεν μπορούν με κανένα τρόπο να αποδοθούν σε ένα υποκείμενο των δεδομένων χωρίς την χρήση συμπληρωματικών πληροφοριών. Ο Κανονισμός αναφέρει ρητά ότι αυτές οι συμπληρωματικές πληροφορίες πρέπει να διατηρούνται ξεχωριστά και να υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Επίσης ο Κανονισμός αναφέρει ρητά ότι τα ψεδωνυμοποιημενα δεδομένα δεν πρέπει να θεωρούνται ανώνυμα αλλά πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο.

Συγκατάθεση: Είναι μια ενέργεια με την οποία το υποκείμενο των δεδομένων συμφωνεί στην επεξεργασία των δεδομένων που τον αφορούν. Η συγκατάθεση ωστόσο θα πρέπει να είναι ελεύθερη, συγκεκριμένη, ρητή και να είναι πάντα με πλήρη επίγνωση του υποκείμενου των δεδομένων.

2.3.2 Άρθρο 13 – Πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων

Ο σκοπός του άρθρου αποτελεί η διαφάνεια και η ενημέρωση του υπεύθυνου επεξεργασίας προς το υποκείμενο των δεδομένων. Συγκεκριμένα ορίζει ότι εφόσον ο υπεύθυνος επεξεργασίας συλλέγει δεδομένα προσωπικού χαρακτήρα από το υποκείμενο των δεδομένων, ο πρώτος οφείλει να παρέχει στον δεύτερο την ταυτότητά του και τα στοιχεία επικοινωνίας του όπως και τον σκοπό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα καθώς και τους αποδέκτες αυτών των δεδομένων. Επιπρόσθετα ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων και τις ακόλουθες επιπλέον πληροφορίες: το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα, τη δυνατότητα του υποκειμένου των δεδομένων να διορθώσει ή να διαγράψει τα δεδομένα προσωπικού χαρακτήρα ή ακόμα και να περιορίσει την επεξεργασία που θα κάνει ο υπεύθυνος επεξεργασίας. Επίσης ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο των δεδομένων ότι έχει τη δυνατότητα να ανακαλέσει οποτεδήποτε την συγκατάθεση του για επεξεργασία των δεδομένων προσωπικού χαρακτήρα όπως και το δικαίωμά του να προβεί σε καταγγελία στην εποπτική αρχή εφόσον υπάρξει παραβίαση των ανωτέρω.

2.3.3 Άρθρο 22 – Δημιουργία Προφίλ

Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ όπως αναφέρεται στο άρθρο 22 του Κανονισμού, είναι οποιαδήποτε μορφή αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που προέρχονται από διάφορες συσκευές με σκοπό την αξιολόγηση ορισμένων πτυχών ενός ατόμου και την λήψη καλύτερων αποφάσεων χωρίς την γνώση ή την συγκατάθεση αυτού.

Η πρόοδος της τεχνολογίας σε συνάρτηση με την ραγδαία αύξηση των συσκευών Internet of Things (IoT), αλλά και την ανάπτυξη του τομέα της τεχνητής νοημοσύνης (AI) και νευρωνικών δικτύων (neural networks) παράλληλα με την ευρεία χρήση των κοινωνικών δικτύων (social networks), έκανε την αυτόματη δημιουργία προφίλ όπως και την λήψη αποφάσεων πολύ εύκολη. Οι δυνατότητες αυτές μπορούν, εφόσον έχουν συλλεγεί τα κατάλληλα δεδομένα, να προβλέψουν την συμπεριφορά, συνήθειες αλλά και διάφορες πτυχές ενός ατόμου. Ωστόσο επηρεάζουν σε μεγάλο βαθμό τα δικαιώματα και τις ελευθερίες των ατόμων.

Ένα χαρακτηριστικό, πρόσφατο, παράδειγμα είναι το σκάνδαλο της Cambridge Analytica[3] στο οποίο η εν λόγω εταιρία χρησιμοποιούσε το Facebook για να συλλέγει δεδομένα από εκατομμύρια χρήστες, χωρίς την συγκατάθεσή τους (μάλιστα, χωρίς ούτε να ενημερώνονται σχετικώς), τα οποία μέσω διαφόρων αυτοματοποιημένων επεξεργασιών κατανέμηναν τους χρήστες σε κατηγορίες, όπου μετά χρησιμοποιούσαν άλλα μέσα όπως διαφημίσεις ή Fake news για να στρέψουν την άποψη τους σε αυτή που ήθελαν. Η εν λόγω εταιρία χρηματοδοτήθηκε και μεταξύ άλλων από τον Trump κατά την προεκλογική του εκστρατεία.

Άλλα παραδείγματα για αυτό μπορούν να υπάρχουν στον τραπεζικό τομέα, στην υγειονομική περίθαλψη, στην ασφάλιση, στο μάρκετινγκ και στις διαφημίσεις. Με άλλα λόγια ο υπεύθυνος επεξεργασίας, για παράδειγμα ο ασφαλιστής, συλλέγει πληροφορίες για το υποκείμενο των δεδομένων, τον ασφαλιζόμενο που θα ασφαλίσει, όπως την κατάσταση υγείας του, πόσες ώρες δουλεύει, τον μισθό του, τι κάνει στον ελεύθερο του χρόνο κ.α. τα οποία εισάγονται σε ένα υπολογιστικό σύστημα και αυτό αποφασίζει τι ασφάλιση θα του κάνει. Εάν θα γίνει αυτό, όπως αναφέρει το άρθρο, ο ασφαλιζόμενος

[3] https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html

πρέπει να το γνωρίζει και να δώσει την συγκατάθεσή του. Έχει κάθε δικαίωνα να αρνηθεί την απόφαση της αυτοματοποιημένης επεξεργασίας δεδομένων.

2.3.4 Άρθρο 25 - Προστασία Δεδομένων από Σχεδιασμό και εξ Ορισμού

Όπως αναφέρει στην αιτιολογική σκέψη 78 σε σχέση με το εν λόγω άρθρο, ο υπεύθυνος επεξεργασίας, κατά την φάση του σχεδιασμού των συστημάτων επεξεργασίας, πρέπει να εφαρμόζει, αλλά και να μπορεί να αποδείξει, την λήψη κατάλληλων μέτρων και χρησιμοποίηση μεθόδων ενίσχυσης της ιδιωτικότητας. Για την σωστή σχεδίαση πρέπει να λάβει υπόψη τις τελευταίες εξελίξεις τις τεχνολογίας, την φύση και τον σκοπό της επεξεργασίας όπως και τους πιθανούς κινδύνους που εγκυμονούν κατά των δικαιωμάτων και των ελευθεριών του υποκείμενου των δεδομένων από την επεξεργασία. Αυτό είναι σημαντικό να γίνεται έγκαιρα, κατά το σχεδιασμό/ανάπτυξη του συστήματος που θα συντελέσει την επεξεργασία, και όχι εκ των υστέρων.

Επίσης ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι κατά τη φάση της επεξεργασίας δεδομένων εφαρμόζεται, εξ' ορισμού, επεξεργασία των δεδομένων προσωπικού χαρακτήρα που είναι αναγκαία μόνο για τον σκοπό της επεξεργασίας αλλά και ότι δεν θα καθίστανται προσβάσιμα χωρίς την συγκατάθεση του υποκείμενου των δεδομένων σε τρίτους. Αυτή η υποχρέωση ισχύει για όλο το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται από την στιγμή που συλλέγονται μέχρι και την διαγραφή τους.

2.3.5 Άρθρο 32 - Ασφάλεια Επεξεργασίας

Σε αυτό το άρθρο καθορίζονται οι υποχρεώσεις του υπεύθυνου επεξεργασίας αλλά και του εκτελούντος την επεξεργασία εφόσον. Έχουν και οι δύο την ευθύνη να λάβουν όλα τα τεχνικά και οργανωτικά μέτρα για να διασφαλίσουν το απαραίτητο επίπεδο ασφάλειας έναντι των κινδύνων που απειλούν τα προσωπικά δεδομένα. Αυτά τα μέτρα θα πρέπει να περιλαμβάνουν κατά περίπτωση – λαμβάνοντας υπόψη τη φύση της επεξεργασίας, τις συνέπειες που θα υπάρξουν για τα υποκείμενα των δεδομένων σε περίπτωση παραβίασης ασφάλειας, το κόστος κτλ. – τα εξής (όχι αποκλειστικά):

- Ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα.

- Να μπορεί να διασφαλιστεί το απόρρητο, την ακεραιότητα, η διαθεσιμότητα και η αξιοπιστία των συστημάτων σε συνεχή βάση. Με αυτό το μέτρο ο υπεύθυνος επεξεργασίας αλλά και ο εκτελών την επεξεργασία είναι υποχρεωμένοι να προστατεύουν τα δεδομένα αυτά από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση ή διαρροή αλλά επίσης να είναι σε θέση να διαθέτουν τα συστήματά τους στο χρήστη απρόσκοπτα.
- Να μπορεί να γίνει αποκατάσταση της διαθεσιμότητας σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού προβλήματος.

Να έχει σχεδιαστεί μια διαδικασία στην οποία θα αξιολογείται η αποτελεσματικότητα των τεχνικών και οργανωτικών μέτρων που λήφθηκαν, έτσι ώστε να μπορεί να διασφαλιστεί αλλά και να αξιολογηθεί η ασφάλεια της επεξεργασίας κατά τακτά χρονικά διαστήματα.

Κεφάλαιο 3

Θέματα Ιδιωτικότητας και προστασίας δεδομένων στις έξυπνες συσκευές και εφαρμογές

3.1 Γενικά

Η τεχνολογική πρόοδος προσφέρει όλο και περισσότερα μέσα για την υποστήριξη του τρόπου ζωής του κάθε ανθρώπου, όπως συσκευές προσδιορισμού θέσης, έξυπνα ρολόγια ή συσκευές παρακολούθησης φυσικής κατάστασης. Όλα έχουν σκοπό την ευκολία και την απλούστευση της ζωής των χρηστών τους, αφού συλλέγονται δεδομένα του τρόπου ζωής των χρηστών και παρουσιάζονται σε αυτούς δίνοντας λύσεις ή και στατιστικά στοιχεία που δεν θα ήταν δυνατό να προσδιοριστούν στο παρελθόν. Ωστόσο ο έλεγχος του βαθμού επέμβασης στην ιδιωτικότητα τον οποίο πραγματοποιούν όλες αυτές οι συσκευές/εφαρμογές γίνεται όλο και πιο περίπλοκος, ενώ παράλληλα εγκυμονεί όλο και περισσότερους κινδύνους η απώλεια τέτοιων δεδομένων από τρίτους.

3.2 Παράγοντες που αποτελούν ρίσκο στην ιδιωτικότητα

Εδώ θα αναλυθούν παράγοντες που αποτελούν ρίσκο για την ιδιωτικότητα ενός χρήστη.

3.2.1 Ποικιλία δεδομένων και πολλαπλοί αισθητήρες

Οι κινητές συσκευές συνήθως έχουν πρόσβαση σε διαφόρους τύπους προσωπικών δεδομένων (δεδομένα υγείας, ευημερίας, ιατρικά δεδομένα) που παρέχονται κατευθείαν από τον χρήστη μέσω των διαφόρων εφαρμογών. Παράλληλα η ενσωμάτωση όλο και περισσότερων αισθητήρων (κάμερα, μικρόφωνο, gps, επιταχυνσιόμετρο, κ.α.) ευκολύνει την δημιουργία δεδομένων και μεταδεδομένων που μπορεί να προκαλέσουν απροσδόκητες επιπτώσεις στην ιδιωτικότητα του χρήστη. Ένα παράδειγμα αποτελεί η έρευνα (M. Gadaleta and Rossi 2018) που αποδεικνύει ότι ένας χρήστης μπορεί να εντοπιστεί και να πιστοποιηθεί από τον τρόπο κίνησης του δηλαδή τον τρόπο που περπατάει.

3.2.2 Συσκευή ως επέκταση του χρήστη

Πλέον η πλειοψηφία των χρηστών βλέπει την προσωπική τους συσκευή ως επέκταση του εαυτού τους, και τείνουν να την θεωρούν αξιόπιστη και πολύ προσωπική. Παράλληλα όμως οι συσκευές είναι σχεδόν πάντα ενεργοποιημένες και μεταφέρονται από τον χρήστη τους σχεδόν παντού όπου και συνδέονται με διάφορα δίκτυα. Συνήθως αποθηκεύουν πολλά προσωπικά δεδομένα του χρήστη και για αρκετό καιρό. Αυτό βέβαια καθιστά τις συσκευές αυτές τέλειους στόχους σε διαφημίσεις αλλά άτομα που αναλύουν δεδομένα όπως ορίζει ο όρος «liquid surveillance» (Z. Bauman and Lyon 2013) όπου εντοπίζονται και καταγράφονται ακόμα και τα μικρότερα στοιχεία της καθημερινότητας του χρήστη.

3.2.3 Τύποι αναγνωριστικών

Κάθε κινητή συσκευή ανάλογα από το λειτουργικό σύστημα που έχει, περιέχει πολλούς και διαφορετικούς τύπους αναγνωριστικών (J. P. Achara et al. 2016) ή δακτυλικά αποτυπώματα που μπορούν να χρησιμοποιηθούν από εφαρμογές για τον εντοπισμό και παρακολούθηση του κάθε χρήστη. Σε αυτό τον τομέα έγιναν πολλές έρευνες όπως (Y. A. de Montjoye et al. 2013) που δείχνει ότι 4 χωροχρονικά σημεία που ενδεχομένως να προήλθαν από τους αισθητήρες μιας κινητής συσκευής είναι αρκετά να ταυτοποιήσουν ένα χρήστη με πιθανότητα 95%.

3.2.4 Εντοπισμός και εξαγωγή προφίλ

Κάθε κινητή συσκευή μπορεί να εντοπιστεί γεωγραφικά αλλά και να παρακολουθείται. Αυτό το γεγονός επιφέρει αρκετούς κινδύνους στην ιδιωτικότητα του κάθε χρήστη, όπως για παράδειγμα να εξάγονται ευαίσθητα προσωπικά δεδομένα όπως η θρησκεία του

χρήστη ή ενδεχομένως ασθένειες που πάσχει αποτέλεσμα των επισκέψεων του σε χώρους λατρείας ή νοσοκομεία και κλινικές. Παράλληλα μπορεί να παρακαλουθούνται οι συσκευές από τρίτους στο διαδίκτυο, εφόσον συνδεθεί η συσκευή σε αυτό, όπου οι τρίτοι μπορεί να συνδυάζουν δεδομένα από διάφορα third party libraries για την ολοκληρωμένη εξαγωγή προφίλ για τον κάθε χρήστη (D. Arp et al. 2017).

3.2.5 Υπέρμετρη συλλογή δεδομένων

Χρόνο με χρόνο οι δυνατότητες και η επίδοση των κινητών συσκευών μεγαλώνει. Ενσωματώνουν καινούριους αισθητήρες και ανακαλύπτονται καινούριοι τρόποι για συλλογή όλο και περισσότερων δεδομένων. Οι εφαρμογές αναβαθμίζονται για να κάνουν χρήση όλων των καινούριων αισθητήρων και μεθόδων συλλογής δεδομένων με σκοπό την καλύτερη ανάλυση ή την πιο αποτελεσματική λειτουργία των υπηρεσιών που προσφέρουν. Ωστόσο αυτό έχει και σαν αποτέλεσμα ότι με την απαγόρευση χρήσης ενός αισθητήρα από την εφαρμογή να μην επιτρέπει την λειτουργία της ή να περιορίζει αρκετά τις υπηρεσίες που προσφέρει, εξαναγκάζοντας έτσι τον χρήστη να δίνει πρόσβαση σε όλους τους αισθητήρες που θέλει η εφαρμογή. Με αυτό τον τρόπο οι εφαρμογές συλλέγουν υπέρμετρα δεδομένα προσωπικού χαρακτήρα από τους χρήστες και συχνά αυτά αποθηκεύονται σε third party libraries.

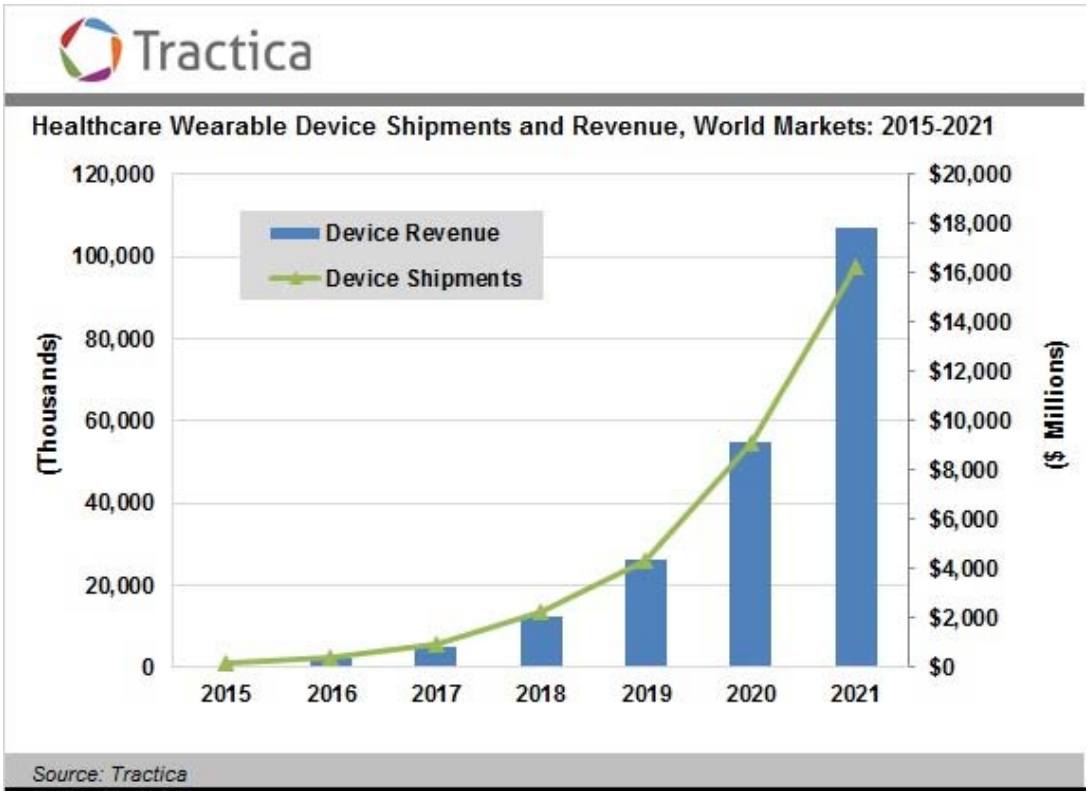
Κεφάλαιο 4

Πλαίσιο της έρευνας

4.1 Τι είναι συσκευή παρακολούθησης φυσικής κατάστασης

Συσκευές παρακολούθησης της φυσικής κατάστασης ή Fitness Trackers ή Activity Trackers αποτελούν μια κατηγορία wearables που τα τελευταία χρόνια παρουσιάζει ραγδαία ανάπτυξη (βλ. Διάγραμμα 1). Είναι κομψά και διακριτικά wearables τα οποία συνοδεύουν τον χρήστη 24 ώρες το 24ωρο και καταγράφουν κάθε του κίνηση. Εφόσον χρησιμοποιούνται σωστά, βοηθούν τον χρήστη να υιοθετήσει ένα πιο υγιεινό τρόπο ζωής, να θέσει στόχους και να τον βοηθήσει να τους πετύχει κάνοντας ταυτόχρονα και την καθημερινή του γυμναστική.

Κάθε wearable συσκευή έχει μια εφαρμογή που συγχρονίζεται μαζί της έτσι ώστε να μπορεί να λαμβάνει αυτή η εφαρμογή τα «ακατέργαστα» δεδομένα που συλλέγει η συσκευή και να τα επεξεργάζεται προκειμένου να παρουσιάζει στον χρήστη τα αποτελέσματα της ημέρας ή της άσκησης και να βγάζει συμπεράσματα μέσα από αυτά. Συνήθως αυτά τα δεδομένα δεν αποθηκεύονται στην εφαρμογή, αλλά ανεβαίνουν σε διακομιστές (servers) της εταιρίας που τα διαχειρίζεται.



Διάγραμμα 1. Παρουσίαση των συνολικών πωλήσεων σε Fitness Trackers όπως και τα έσοδα από αυτά σε παγκόσμια κλίμακα. [4]

Πολλές φορές οι εταιρίες θέλοντας να δείξουν την δραστηριότητα των χρηστών τους παρουσιάζουν, ανώνυμα μεν, δεδομένα. Μια από αυτές τις περιπτώσεις είναι η Strava η οποία δημιούργησε το Heatmap στο οποίο απεικονίζει τις δραστηριότητες των χρηστών της (δημόσιες μόνο, όχι ιδιωτικές) σε χάρτη. Μέσω αυτού όμως, αποκαλύφθηκαν μυστικές στρατιωτικές βάσεις σε Συρία, Ιράκ, Αφγανιστάν, αφού οι στρατιώτες έκαναν χρήση τέτοιων συσκευών (βλ. Εικόνα 1).

[4] https://www.tractica.com/newsroom/press-releases/healthcare-wearable-device-shipments-to-reach-98-million-units-annually-by-2021/

Εικόνα 1. Στρατιωτική Βάση στην επαρχία Χέλμανς στο Αφγανιστάν. Τα δρομολόγια δημιουργήθηκαν από δρομείς μέσω της εφαρμογής Strava. [5]

Κάθε μια από αυτές τις συσκευές είναι εφοδιασμένη με πολλούς αισθητήρες. Οι πιο συνήθεις αισθητήρες που παρατηρούνται είναι επιταχυνσιόμετρο 3 διευθύνσεων (3-way accelerometer), γυροσκόπιο, αλτίμετρο και οπτικό μετρητή καρδιακού παλμού. Μέσω των raw δεδομένων που προκύπτουν από τους αισθητήρες αλλά και την επεξεργασία με ειδικούς αλγόριθμους παρουσιάζουν στον χρήστη τα ημερήσιά του βήματα, διάφορες αθλητικές δραστηριότητες όπως τρέξιμο, ποδηλασία, κολύμπι κ.α, ιστορικό ύπνου, μετρήσεις καρδιακών παλμών κτλ.

4.2 Εφαρμογές και Συσκευές που Επιλέχτηκαν

Για την επίτευξη των ερευνητικών στόχων της παρούσας μεταπτυχιακής διατριβής, επιλέχθηκαν 6 διαφορετικές εφαρμογές που περιγράφονται πιο κάτω, και οι οποίες εγκαταστάθηκαν και «εκτελέστηκαν» σε 4 ξεχωριστές συσκευές όπως περιγράφεται στον πίνακα στη συνέχεια:

[5] https://www.strava.com/heatmap

Α/Α	Όνομα Εφαρμογής	Συσκευή Συλλογής Δεδομένων	Κινητό τηλέφωνο/ Έκδοση Android
1	Google Fit	Αισθητήρες του κινητού	Samsung Galaxy S6 Edge (Android 7.0)
2	Samsung Health	Αισθητήρες του κινητού	Samsung Galaxy S6 Edge (Android 7.0)
3	LG Health	Αισθητήρες του κινητού	Samsung Galaxy S6 Edge (Android 7.0)
4	Mi Fit	Xiaomi Mi Band 3	Samsung Galaxy S6 Edge (Android 7.0)
5	Huawei Health	Huawei Honor Band 4	Samsung Galaxy S6 Edge (Android 7.0)
6	Garmin Connect	Garmin Fenix 2	Samsung Galaxy S6 Edge (Android 7.0)

Πίνακας 1. Παρουσίαση των εφαρμογών που ερευνήθηκαν και την συσκευή μέσω της οποίας αντλήθηκαν τα δεδομένα από τον χρήστη.

Οι πιο πάνω εφαρμογές επιλέχθηκαν με κριτήριο την δημοτικότητα των κατασκευαστριών εταιριών αφού είναι οι μεγαλύτερες στην κατηγορία των Android smartphone[6] (Samsung, Huawei, Xiaomi, LG, Google), ενώ η εφαρμογή της Garmin επιλέχθηκε διότι η εταιρία αποτελεί μια εκ των μεγαλύτερων σε δημοτικότητα και πωλήσεις smartwatch. Επίσης όλες αυτές οι εφαρμογές μπορούν να χρησιμοποιηθούν στις πλειοψηφία των συσκευών Android και iOS. Όσο αφορά τις wearable συσκευές, αποτελούν την μέθοδο συλλογής δεδομένων και συγχρονίζονται μόνο με την εφαρμογή του κατασκευαστή τους.

4.2.1 Google Fit[7]

Η εφαρμογή αυτή επιλέχτηκε διότι η Google αποτελεί την μεγαλύτερη εταιρία όσον αφορά τις διαφημίσεις αλλά και την διαχείριση δεδομένων, έχοντας πρωτοποριακές και εξειδικευμένες μεθόδους για συλλογή πληροφοριών από τους χρήστες της. Παράλληλα έχει όλες τις δυνατότητες που έχουν οι εφαρμογές αυτού του είδους σήμερα, δηλαδή μέτρηση

[6] https://www.appbrain.com/stats/top-manufacturers
[7] https://play.google.com/store/apps/details?id=com.google.android.apps.fitness

βημάτων, καρδιακών παλμών, αυτόματη εντόπιση δραστηριότητας όπως περπάτημα, τρέξιμο, ποδήλατο, κολύμβηση, κα. Μπορεί να εγκατασταθεί σε όλες τις συσκευές Android ή IOS αλλά και σε wearable συσκευές Android Wear.

4.2.2 Samsung Health[8]

Η επόμενη εφαρμογή που επιλέχθηκε είναι το Samsung Health. Ο λόγος που επιλέχθηκε είναι επειδή η Samsung ξεκίνησε να προεγκαθιστά την εφαρμογή αυτή πάνω σε ορισμένα κινητά τηλέφωνα μετά το 2013. Σύμφωνα με την εταιρία τον Σεπτέμβρη του 2018 είχε περισσότερους από 65εκ ενεργούς χρήστες[9] κάνοντας την εφαρμογή ως μια από τις πιο δημοφιλείς στον τομέα αυτό. Η εφαρμογή αυτή χρησιμοποιεί τα sensors του smartphone για την συλλογή δεδομένων, όπου αυτά στην συνέχεια επεξεργάζονται με ειδικούς αλγόριθμους της εταιρίας και στην συνέχεια παρουσιάζονται στον χρήστη. Μεταξύ άλλων εκτός από τις συνήθεις δυνατότητες των εφαρμογών αυτών μπορεί να καταγράψει τα γεύματα του χρήστη, τον ύπνο, το νερό που καταναλώνει, τους καφέδες κ.α.

4.2.3 LG Health[10]

Το LG Health επιλέχθηκε ως μια εφαρμογή εφάμιλλη με αυτή της Samsung. Έρχεται και αυτή προεγκατεστημένη σε ορισμένα κινητά της LG από το 2014. Είναι επίσης διαθέσιμη και από το Google Play Store. Όπως και στο Samsung Health έτσι και αυτή χρησιμοποιεί τα sensors του smartphone για την συλλογή δεδομένων. Οι δυνατότητες της εφαρμογής μπορούν να χαρακτηριστούν ως βασικές αφού μόνο μετρά βήματα και καταγράφει τις δραστηριότητες του χρήστη. Δυστυχώς δεν έχει την ανάλογη υποστήριξη και πολλοί χρήστες, με βάση τις δημοσιευμένες αξιολογήσεις[10], είναι δυσαρεστημένοι με προβλήματα που υπάρχουν.

4.2.4 Mi Fit[11]

Η εφαρμογή αυτή είναι η αντίστοιχη της Huami (θυγατρική της Xiaomi). Ως μια από τις κορυφαίες εταιρίες της Κίνας κρίθηκε ότι είναι σημαντικό να συμπεριληφθεί στη μελέτη. Η Xiaomi έχει καταφέρει να γίνει ο μεγαλύτερος προμηθευτής wearable συσκευών,

[8] https://play.google.com/store/apps/details?id=com.sec.android.app.shealth
[9] https://news.samsung.com/global/samsung-announces-latest-updates-to-samsung-health-for-a-more-interactive-and-personalized-health-and-wellness-experience
[10] https://play.google.com/store/apps/details?id=com.lge.lifetracker
[11] https://play.google.com/store/apps/details?id=com.xiaomi.hm.health

ξεπερνώντας την Fitbit και την Apple το 2018[12]. Επίσης ένα από τα τελευταία της επιτεύγματα ήταν πουλήσουν περισσότερα από 1 εκ Mi Band 4 σε μόλις 8 ημέρες ενώ το περσινό Mi Band 3 με 23,3 εκ πωλήσεις κατείχε το 13,5% της αγοράς fitness trackers![13] Η επιτυχία αυτή οφείλεται στις πολύ χαμηλές τιμές που προσφέρει η Xiaomi τα προϊόντα της, τα οποία είναι κατά πολύ φθηνότερα από τα υπόλοιπα προϊόντα της αγοράς στον συγκεκριμένο τομέα. Όσο αφορά την εφαρμογή, δεν χρησιμοποιεί το κινητό σαν συσκευή για να μαζέψει δεδομένα, αλλά συγχρονίζεται με άλλες wearable συσκευές της Xiaomi και αντλεί, αναλύει και επεξεργάζεται δεδομένα από αυτές.

4.2.5 Huawei Health[14]

Η αντίστοιχη εφαρμογή της Huawei έχει ακριβώς τις ίδιες δυνατότητες με αυτή της Xiaomi. Η εταιρία τον τελευταίο καιρό βρίσκει τις ΗΠΑ και άλλα κράτη εναντίον της, ισχυριζόμενα ότι η εταιρία χρησιμοποιεί τα προϊόντα της για να μαζεύει πληροφορίες από τους χρήστες και να τα δίνει στην κυβέρνηση της Κίνας[15]. Η εφαρμογή όπως και της Xiaomi βασίζεται πάνω σε wearable συσκευές της ίδιας εταιρίας για συλλογή δεδομένων, που συγχρονίζονται με αυτή και αναλύει και επεξεργάζεται δεδομένα από αυτές. Εδώ θα πρέπει να αναφερθεί ότι για την λειτουργία της εφαρμογής σε οποιοδήποτε smartphone εκτός αυτά της Huawei θα πρέπει ο χρήστης να εγκαταστήσει την εφαρμογή Huawei Mobile Services[16] από το Play Store.

4.2.6 Garmin Connect[17]

Η Garmin είναι μια Αμερικάνικη εταιρία τεχνολογίας με εξειδίκευση στις τεχνολογίες GPS που είναι πολύ δημοφιλής στην Ευρώπη και Αμερική. Η εταιρία προσφέρει ένα μεγάλο εύρος από ρολόγια πολλαπλών ρόλων, τα οποία μπορούν να χρησιμοποιηθούν και για γυμναστική. Η εφαρμογή της εταιρίας, όπως και οι προηγούμενες, συγχρονίζεται με αυτές τις συσκευές και μαζεύει και αναλύει τα δεδομένα του χρήστη, τα οποία αφού τα επεξεργάζεται τα παρουσιάζει σε αυτόν.

[12] https://www.telegraph.co.uk/technology/2018/12/04/chinas-xiaomi-takes-lead-apple-top-seller-wearable-technology/
[13] https://www.phonearena.com/news/Xiaomi-sells-1-million-Mi-Band-4-units-in-8-days_id117051
[14] https://play.google.com/store/apps/details?id=com.huawei.health
[15] https://www.theguardian.com/commentisfree/2018/dec/28/huawei-west-trade-war-tech-china-shenzhen
[16] https://play.google.com/store/apps/details?id=com.huawei.hwid&hl=en_US
[17] https://play.google.com/store/apps/details?id=com.garmin.android.apps.connectmobile

4.3 Διερεύνηση Ιδιωτικότητας και Ασφάλειας

Στο τμήμα αυτό μελετάται η πολιτική απορρήτου (γνωστή επίσης και με τον όρο πολιτική ιδιωτικότητας), όπως αναρτήθηκε από την κάθε υπηρεσία, η οποία και (οφείλει να) καταγράφει τι δεδομένα συλλέγουν καθώς και για ποιους σκοπούς. Όπου μπορούσε να επιλεγεί χώρα για την πολιτική απορρήτου επιλεγόταν η Κύπρος. Όταν δεν υπήρχε ως επιλογή η Κύπρος επιλεγόταν η Ελλάδα ή άλλη χώρα εντός της Ευρωπαϊκής Ένωσης. Οι εν λόγω πολιτικές εξετάστηκαν στις 08/09/2019.

4.3.1 Google Fit (Τελευταία ενημέρωση Privacy Policy: 22 Ιαν 2019) (Google 2019)

Η εφαρμογή Google Fit δεν έχει ξεχωριστή πολιτική απορρήτου αλλά παραπέμπει στην πολιτική απορρήτου της Google γενικά. Μέσα από αυτή δεν ξεχωρίζει τι δεδομένα συλλέγονται αναλυτικά από κάθε εφαρμογή ή υπηρεσία της Google αλλά αναφέρει συνολικά τι συλλέγονται από όλες τις υπηρεσίες και εφαρμογές, καθιστώντας έτσι αδύνατο να εξακριβωθεί τι πληροφορία συλλέγεται επακριβώς και πώς αυτή χρησιμοποιείται.

4.3.2 Samsung Health (Τελευταία ενημέρωση Privacy Policy: 17 Οκτ 2018) (Samsung 2018)

Α. Δεδομένα που συλλέγονται από την συσκευή:

- Δεδομένα του χρήστη όπως email, ονοματεπώνυμο, χώρα, ταχυδρομικό κώδικα, username και ID του Samsung Health και φωτογραφία προφίλ.
- Λοιπά δεδομένα του χρήστη όπως ημερομηνία γέννησης, φύλο.
- Δεδομένα που σχετίζονται με τη φυσική κατάσταση ή/και την υγεία όπως ύψος, βάρος, φυσική δραστηριότητα, καρδιακούς παλμούς και μεταβολισμό.
- Δεδομένα άσκησης και δίαιτας όπως έκταση και φύση της σωματικής δραστηριότητας, και δεδομένα κατάποσης και γευμάτων.
- Αλληλεπιδράσεις με το Samsung Health όπως πληροφορίες σχετικά με τη χρήση της εφαρμογής, συμπεριλαμβανομένων των μηνυμάτων που αποστέλλονται ή λαμβάνονται, ρυθμίσεις της εφαρμογής και δεδομένα εσωτερικής χρήσης της εφαρμογής (μενού και επιλεγμένες ρυθμίσεις, χαρακτηριστικά που χρησιμοποιούνται, συχνότητα και διάρκεια χρήσης), και τυχόν μηνύματα σφάλματος που ενδέχεται να εμφανιστούν. Επίσης συλλέγονται άλλα δεδομένα σχετικά με τη χρήση της εφαρμογής, συμπεριλαμβανομένων δεδομένων όπως τις εφαρμογές που

χρησιμοποιεί ο χρήστης, τους ιστότοπους που επισκέπτεται, τις λίστες επαφών του, εικόνες, τραγούδια, καταχωρήσεις ημερολογίου, σελιδοδείκτες, σημειώσεις, ρυθμίσεις ξυπνητηριού, περιεχόμενο και δεδομένα από άλλες εφαρμογές της Samsung και τρίτων κατασκευαστών, ιστότοπων και υπηρεσιών που λαμβάνονται από τη Samsung και από εφαρμογές και υπηρεσίες τρίτων κατασκευαστών.

- Δεδομένα γεωγραφικής θέσης. Με τη συγκατάθεση του χρήστη, λαμβάνονται σήματα GPS, Bluetooth και Wi-Fi και άλλες τεχνολογίες.
- Δεδομένα συσκευής και εφαρμογής. Χρησιμοποιούνται αυτοματοποιημένες διαδικασίες για να συλλεχθούν πληροφορίες σχετικά με τις συσκευές του χρήστη που είναι συνδεμένες με το Samsung Health, όπως και δεδομένα συσκευών, συμπεριλαμβανομένων των αναγνωριστικών, την έκδοση λογισμικού της συσκευής και την έκδοση της εφαρμογής.
- Συσκευές και εφαρμογές τρίτων κατασκευαστών. Συλλέγονται πληροφορίες σχετικά με εφαρμογές που συνδέονται με την εφαρμογή Samsung Health. Αυτές οι πληροφορίες περιέχουν τον κατασκευαστή της συσκευής, μοντέλο και αναγνωριστικά, καθώς και αναγνωριστικά εφαρμογών, συμπεριλαμβανομένων των αναγνωριστικών εφαρμογών κοινωνικών μέσων.
- Δεδομένα των κοινωνικών μέσων. Συλλέγονται πληροφορίες κοινωνικών μέσων, όπως μηνύματα που στέλνονται ή λαμβάνονται στην εφαρμογή, δημοσιεύσεις, συγχαρητήρια μηνύματα, σχόλια και απαντήσεις στην κοινότητα.

Β. Σκοπός των δεδομένων που συλλέγονται:

- Για την παροχή υπηρεσιών όπως δημιουργίας αντιγράφων ασφαλείας και συγχρονισμού.
- Για να προσδιορίζεται και πιστοποιείται η ταυτότητα του χρήστη.
- Για να βελτιώνεται και προσαρμόζεται η εμπειρία του χρήστη στις υπηρεσίες της εφαρμογής.
- Για διεξαγωγή, αξιολόγηση και βελτίωση των επιχειρησιακών διαδικασιών.
- Για την προστασία από απάτες και άλλες εγκληματικές δραστηριότητες, αξιώσεις και άλλες ευθύνες.
- Για την επικοινωνία με τον χρήστη μέσω των προϊόντων και των υπηρεσιών της εφαρμογής για διαφημιστικούς σκοπούς (μπορεί να απενεργοποιηθεί).

Γ. Λοιπές πληροφορίες:

- Η εταιρία επεξεργάζεται προσωπικά δεδομένα μόνο όταν είναι ανάγκη για την παροχή συγκεκριμένων υπηρεσιών και την βελτίωση αυτών, για την εκτέλεση μιας ενέργειας όπως να απαντήσουν σε μια ερώτηση του χρήστη και όταν απαιτείται για τα νόμιμα συμφέροντα της εταιρίας είτε είναι για περεταίρω παροχή πληροφοριών σχετικά με προϊόντα και υπηρεσίες είτε για την προστασία του χρήστη.
- Δεν αποκαλύπτονται προσωπικά δεδομένα των χρηστών με υπηρεσίες εκτός από τις περιπτώσεις που ορίζονται στην Πολιτική Απορρήτου.
- Λαμβάνονται μέτρα για να διασφαλιστεί ότι οι πληροφορίες σχετικά με τους χρήστες διατηρούνται μόνο για την περίοδο κατά την οποία χρησιμοποιούνται τα δεδομένα για την παροχή της υπηρεσίας, όπως απαιτείται από το νόμο, και μόνο για όσο χρονικό διάστημα είναι απαραίτητο για το σκοπό για τον οποίο συλλέχθηκαν ή υποβλήθηκαν σε επεξεργασία.
- Ο χρήστης έχει ορισμένες επιλογές σε σχέση με τα προσωπικά δεδομένα που θα λαμβάνονται από αυτόν.
- Ο χρήστης έχει το δικαίωμα να ζητήσει λεπτομέρειες σχετικά με τις πληροφορίες που συλλέγονται από αυτόν και να ζητήσει να διορθωθούν τυχόν σφάλματα σε αυτά τα δεδομένα, να αντιταχθεί στην επεξεργασία ή να ζητήσει περιορισμούς στην επεξεργασία, πρόσβαση, διαγραφή ή δυνατότητα μεταφοράς σύμφωνα πάντα με τους νόμους της κάθε χώρας.
- Εφαρμόζονται εύλογα διοικητικά, τεχνικά και φυσικά μέτρα ασφαλείας που αποσκοπούν στην προστασία των Προσωπικών Δεδομένων που λαμβάνονται μέσω των Υπηρεσιών από τυχαία, παράνομη ή μη εξουσιοδοτημένη καταστροφή, παρεμβολές, απώλεια, αλλοίωση, πρόσβαση, αποκάλυψη ή χρήση.

4.3.3 LG Health (Τελευταία ενημέρωση Privacy Policy: 31 Μαρ 2016) (LG 2016)

Η LG όπως αναφέρει στην σελίδα της εφαρμογής στο Play Store, περιορίζει κάποιες λειτουργίες και υπηρεσίες αναλόγως της χώρας που είναι ο χρήστης. Όπως θα παρουσιαστεί και αργότερα η Κύπρος είναι σε αυτές τις χώρες που περιορίζονται αρκετές λειτουργίες με αποτέλεσμα η εφαρμογή να λειτουργεί offline. Όλα τα προσωπικά δεδομένα μένουν στην συσκευή και δεν αποθηκεύονται σε servers ούτε τυγχάνουν επεξεργασίας.

4.3.4 Mi Fit (Τελευταία ενημέρωση Privacy Policy: Δεν αναφέρεται) (Xiaomi n.d.)

Α. Δεδομένα που συλλέγονται από την συσκευή:

- Απαραίτητα προσωπικά δεδομένα που χρειάζονται για να παρέχουν τις υπηρεσίες τους στον χρήστη (δεν αναφέρει κάτι πιο συγκεκριμένο).
- Δεδομένα που χρειάζονται για την δημιουργία του Mi Account όπως email, αριθμός τηλεφώνου, IMEI (International Mobile Equipment Identity) και διάφορες τοπικές πληροφορίες όπως κωδικός χώρας και δίκτυο κινητής τηλεφωνίας.
- Κατά την δημιουργία του Mi Account δεδομένα όπως ηλικία, ύψος, βάρος και φύλο. Προαιρετικά δεδομένα όπως ημερομηνία γεννήσεως, φωτογραφία προφίλ και υπογραφή.
- Κατά τον συγχρονισμό του Fit Band δεδομένα που προκύπτουν από τους αισθητήρες του wearable, όπως δεδομένα ύπνου, δεδομένα κίνησης του χρήστη, δεδομένα καρδιακών παλμών, και έξυπνου ξυπνητηριού.
- Όταν ο χρήστης κοινοποιεί τα δεδομένα του (content) στην οικογένεια ή τους φίλους του, η εφαρμογή ενδέχεται να συλλέξει δεδομένα από αυτούς όπως τα ονόματά τους, την διεύθυνση email τους, το τηλέφωνό τους και την διεύθυνση τους. Επίσης εάν ο χρήστης χρησιμοποιήσει δεδομένα από third parties καθίσταται υπεύθυνος και νοείται ότι έχει την συγκατάθεση για να τα παρέχει αυτά στην εφαρμογή.
- Κατά την επεξεργασία των δεδομένων συλλέγονται δεδομένα όπως το Mi Fit ID, το firmware version, το OS version, το μοντέλο (του smartphone) και το σύστημα, την IP address και την ώρα.

Β. Σκοπός των δεδομένων που συλλέγονται:

- Για την επιβεβαίωση της ταυτότητας του χρήστη, για την εύρυθμη παροχή των υπηρεσιών της εφαρμογής, την εξασφάλιση των διεργασιών και της ασφάλειας αυτών, όπως και την αποφυγή δόλιας και ακατάλληλης χρήσης των υπηρεσιών.
- Για την ανάπτυξη προϊόντων και υπηρεσιών μέσω στατιστικής ανάλυσης.
- Για την επικοινωνία με τον χρήστη.
- Για παρουσίαση στον χρήση μάρκετινγκ και διαφημιστικό υλικό για προϊόντα και υπηρεσίες (υπάρχει δυνατότητα να διαγραφεί αυτή η επιλογή από τον χρήστη)

- Για εξατομίκευση προϊόντων και παροχή υπηρεσιών προσαρμοσμένες πάνω στον χρήστη.
-

Γ. Λοιπές πληροφορίες:

- Χρησιμοποιούνται στατιστικά δεδομένα (ψευδωνυμοποιημένα) για βελτίωση των λειτουργιών και υπηρεσιών που προσφέρονται. Μερικά από αυτά τα δεδομένα είναι γλωσσικές προτιμήσεις, ταχυδρομικός κώδικας, κωδικός χώρας, ζώνη ώρας, επάγγελμα, πληροφορίες σχετικά με την συσκευή (smartphone), γεωγραφικές πληροφορίες, διεύθυνση IP, πρόγραμμα περιήγησης, πηγή αναφοράς (reference source), OS, ημερομηνία, ώρα και καταγραφή των επιλογών (clicks) του χρήστη.
- Παρέχονται παραδείγματα για τον περιορισμό της συλλογής, χρήσης, αποκάλυψης και επεξεργασίας των προσωπικών δεδομένων του χρήστη.
- Ο χρήστης έχει το δικαίωμα να ζητήσει ή να διορθώσει τα προσωπικά του δεδομένα ανάλογα με τους νόμους της κάθε χώρας. Αυτή η πράξη ενδεχομένως να γίνει επί πληρωμής.
- Ο χρήστης έχει το δικαίωμα να ανακαλέσει την συγκατάθεσή του για παροχή των προσωπικών του δεδομένων στην εφαρμογή, ωστόσο αυτό μπορεί να του απαγορεύσει την χρήση των υπηρεσιών της εφαρμογής κατά περίπτωση.
- Όλα τα προσωπικά δεδομένα του χρήστη είναι εμπιστευτικά. Μπορεί να αποκαλυφθούν προσωπικά δεδομένα του χρήστε σε τρίτους εφόσον ο χρήστης ζητήσει συγκεκριμένα προϊόντα ή υπηρεσίες.
- Η εφαρμογή ποτέ δεν θα δώσει τα προσωπικά δεδομένα του χρήστη σε τρίτους χωρίς την συγκατάθεση του χρήστη. Αυτό γίνεται μόνο εφόσον το επιτρέπει ο νόμος σε συγκεκριμένες περιπτώσεις.
- Εφόσον τα προσωπικά δεδομένα θα δοθούν σε τρίτους, με την συγκατάθεση του χρήστη, θα διασφαλιστεί ότι ο τρίτος υπόκειται σε όλες τις υποχρεώσεις που ορίζει ο νόμος προστασίας προσωπικών δεδομένων της κάθε χώρας.
- Επιβεβαιώνεται η χρήση όλων των διαθέσιμων μέσων για την προστασία των προσωπικών δεδομένων από κινδύνους στην ακεραιότητα και διαθεσιμότητα αυτών.

4.3.5 Huawei Health (Τελευταία ενημέρωση Privacy Policy: 30 Μαρ 2019) **(Huawei 2019)**

Α. Δεδομένα που συλλέγονται από την συσκευή:

- Πληροφορίες προσωπικού προφίλ: όπως πληροφορίες λογαριασμού HUAWEI ID (αναγνωριστικό λογαριασμού, εικόνα προφίλ, όνομα χρήστη, φύλο και ημερομηνία γέννησης), ύψος και βάρος.
- Δεδομένα φυσικής κατάστασης: η τοποθεσία της συσκευής σας, ο τόπος άσκησης, ο τύπος άσκησης, η διάρκεια της άσκησης, ο αριθμός των βημάτων, η διανυθείσα απόσταση, η απώλεια θερμίδων, το υψόμετρο, η μέγιστη πρόσληψη οξυγόνου, οι καρδιακοί παλμοί κατά την άσκηση και άλλα δεδομένα ανάλυσης άσκησης θα αποθηκεύονται στο Cloud και θα είναι διαθέσιμα για προβολή στη συσκευή σας.
- Δεδομένα υγείας: Τα δεδομένα που σχετίζονται με τον ύπνο, τους καρδιακούς παλμούς (συμπεριλαμβανομένων των δεδομένων στρες που προκύπτουν από τη μεταβλητότητα των καρδιακών παλμών) και τη σύσταση του σώματος (συμπεριλαμβανομένου του σωματικού λίπους, της ανθεκτικότητας του σώματος, του δείκτη μάζας σώματος, του μεγέθους των μυών, του μεταβολισμού, του ποσοστού νερού στο σώμα, του σπλαχνικού λίπους, των πρωτεϊνών και της οστικής πυκνότητας) θα αποθηκεύονται στο Cloud και θα είναι διαθέσιμα για προβολή στη συσκευή σας.
- Πληροφορίες συσκευής και δικτύου: η διεύθυνση MAC, ο σειριακός αριθμός της συσκευής, το IMEI ή άλλο αναγνωριστικό, ο τύπος της συσκευής, οι ρυθμίσεις της συσκευής και οι προσωπικές σας ρυθμίσεις θα συλλέγονται για τη διαχείριση της συσκευής, συμπεριλαμβανομένων των συνδέσεων Bluetooth, της διαχείρισης διαμόρφωσης της συσκευής, των ενημερώσεων λογισμικού και της εμφάνισης της συσκευής προέλευσης των δεδομένων. Η διεύθυνση IP, ο τύπος δικτύου και η σύνδεση δικτύου θα συλλέγονται επίσης, για τη βελτίωση της εμπειρίας σύνδεσης δικτύου.

Β. Σκοπός των δεδομένων που συλλέγονται:

- Για την παροχή των λειτουργιών του Huawei Health και για την εκπλήρωση συμβατικών υποχρεώσεων.
- Για βελτίωση των υπηρεσιών και της εμπειρίας του χρήστη, με την προϋπόθεση ότι ο χρήστης έχει δώσει τη συγκατάθεσή του για την εν λόγω επεξεργασία δεδομένων.

- Για σκοπούς ασφάλειας πληροφοριών και για την ανίχνευση ή πρόληψη διάφορων τύπων απάτης και κακής χρήσης υπηρεσιών βάσει του έννομου συμφέροντός της εταιρίας.
-

Γ. Λοιπές πληροφορίες:

- Τα δεδομένα υγείας και φυσικής κατάστασης, τα οποία περιλαμβάνουν ευαίσθητες πληροφορίες για εσάς, θα μεταφορτώνονται στο Cloud του Huawei Health μόνο μετά από τη ρητή συγκατάθεσή του χρήστη στην εφαρμογή.
- Η εταιρία θα διατηρεί τα προσωπικά δεδομένα των χρηστών αποκλειστικά για το διάστημα που είναι απαραίτητο για τους σκοπούς που ορίζονται στην δήλωση Απορρήτου. Μετά τη λήξη της περιόδου διατήρησης, θα διαγράφονται ή θα ανωνυμοποιούνται τα προσωπικά δεδομένα σε εύθετο χρόνο, εκτός και αν απαιτείται διαφορετικά από τους νόμους και τους κανονισμούς.
- Ο χρήστης μπορεί να ζητήσει πληροφορίες, καθώς και ένα αντίγραφο των προσωπικών δεδομένων του σε σχέση με το Huawei Health. Επίσης μπορεί να διορθώσει τα δεδομένα του έτσι ώστε να διατηρούνται ενημερωμένα και ακριβή, όπως και να μεταφέρει τα προσωπικά δεδομένα που έχει παράσχει στην εφαρμογή και τα οποία σχετίζονται με το Huawei Health. Τέλος μπορεί ανά πάσα στιγμή να ζητήσει διαγραφή των δεδομένων του.
- Όλες οι συγκαταθέσεις που δόθηκαν για αποθήκευση των δεδομένων υγείας στο Cloud, για επεξεργασία των δεδομένων χρήσης της εφαρμογής και για κοινή χρήση των δεδομένων μπορούν να ανακληθούν.
- Ο χρήστης έχει το δικαίωμα της αντίταξης στην επεξεργασία όπως επίσης και να θέσει υπό περιορισμό την επεξεργασία των δεδομένων.

4.3.6 Garmin Connect (Τελευταία ενημέρωση Privacy Policy: 06 Ιουν 2019) **(Garmin 2019)**

Α. Δεδομένα που συλλέγονται από την συσκευή:

- Κατά την δημιουργία λογαριασμού Garmin συλλέγεται το email και το όνομα του χρήστη. Επιπρόσθετα μπορεί ο χρήστης εφόσον θέλει να δηλώσει τοποθεσία, δραστηριότητες, επίπεδο φυσικής κατάστασης, ώρα ύπνου, ώρα ξυπνήματος, φύλο, ημερομηνία γέννησης, ύψος και βάρος.

- Εάν ο χρήστης επιθυμεί να αποθηκεύονται τα δεδομένα του στους servers της Garmin τότε μπορεί να επιλέξει να μεταφορτώσει δραστηριότητες, δεδομένα δραστηριότητας (π.χ. βήματα, απόσταση, ρυθμός, χρόνος δραστηριότητας, καύσεις θερμίδων, καρδιακοί παλμοί, στατιστικά στοιχεία γκολφ, πληροφορίες για τον κύκλο της εμμήνου ρύσεως, ενυδάτωση, μουσική που παίζεται, κλπ.).
- Όταν συγχρονίζεται μια συσκευή με την εφαρμογή καταγράφονται δεδομένα σχετικά με τη μετάδοση, όπως η διεύθυνση IP που χρησιμοποιείται κατά το συγχρονισμό, η ώρα και η ημερομηνία συγχρονισμού, τα αρχεία καταγραφής / διαγνωστικού ελέγχου, η γεωγραφική θέση της συσκευής, σχετικά με τη συσκευή, πληροφορίες σχετικά με το δίκτυο που χρησιμοποιείται για συγχρονισμό (π.χ. Wi-Fi ή cellular) και το επίπεδο μπαταρίας της συσκευής.
- Όταν θα γίνει επικοινωνία με την Garmin συλλέγονται προσωπικά δεδομένα, όπως το όνομα του χρήστη, το email, ο αριθμός τηλεφώνου, η διεύθυνση, οι προτιμήσεις επικοινωνίας καθώς και πληροφορίες σχετικά με τα προϊόντα της Garmin που έχει στην κατοχή του, όπως serial numbers και ημερομηνίες αγοράς.
- Εάν ο χρήστης επιλέξει να ενώσει τον λογαριασμό του στο Garmin με λογαριασμούς που έχετε σε άλλους παρόχους εφαρμογών, θα λαμβάνονται πληροφορίες σχετικά με τον χρήστη από αυτούς τους λογαριασμούς.

Β. Σκοπός των δεδομένων που συλλέγονται:

- Για την παροχή των υπηρεσιών της εφαρμογής Garmin Connect.
- Για βελτίωση των υπηρεσιών και της εμπειρίας του χρήστη, με την προϋπόθεση ότι ο χρήστης έχει δώσει τη συγκατάθεσή του για την εν λόγω επεξεργασία δεδομένων.
- Για σκοπούς ασφάλειας πληροφοριών και για την ανίχνευση ή πρόληψη διάφορων τύπων απάτης και κακής χρήσης υπηρεσιών βάσει του έννομου συμφέροντός της εταιρίας.
- Για σκοπούς μάρκετινγκ. (προαιρετικό)

Γ. Λοιπές πληροφορίες:

- Οι δραστηριότητες και τα δεδομένα δραστηριότητας που σχετίζονται με τον λογαριασμό Garmin ορίζονται ως "Ιδιωτικά" από προεπιλογή.

- Από καιρό σε καιρό, μοιράζονται ή πωλούνται δεδομένα δραστηριότητας σε τρίτους κατά τρόπο που δεν επηρεάζει τους χρήστες (ανώνυμα δεδομένα), με σκοπό τη βελτίωση της ποιότητας του περιεχομένου ή των λειτουργιών που παρέχουν ή για έρευνα ή άλλους σκοπούς.
- Δεν μοιράζονται προσωπικά δεδομένα σε τρίτους χωρίς την ρητή συγκατάθεση του χρήστη.
- Ο χρήστης έχει το δικαίωμα να ζητήσει από την Garmin πρόσβαση και διόρθωση ή διαγραφή των προσωπικών του δεδομένων. Επίσης έχει το δικαίωμα να αντιταχθεί στην επεξεργασία των προσωπικών του δεδομένων και το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.

4.4 Αποτίμηση των πολιτικών απορρήτου

Εδώ θα πρέπει να τονιστεί ότι όλες οι πολιτικές απορρήτου όλων των υπό αξιολόγηση εφαρμογών (εκτός από την LG και Google) έχουν προσαρμοστεί στην μετέπειτα GDPR εποχή. Ωστόσο ένα γενικό σχόλιο για όλες είναι ότι παρόλο που παρουσιάζουν τον σκοπό επεξεργασίας των δεδομένων, ο σκοπός που παρουσιάζεται είναι πολύ γενικός και δεν περιγράφει ποια δεδομένα χρησιμοποιεί και σε ποια επεξεργασία, πράγμα το οποίο αφήνει ασάφειες ως προς την χρησιμοποίηση των δεδομένων του χρήστη και φυσικά αυτό, κατ' αρχάς, δεν καλύπτει πλήρως τις απαιτήσεις διαφάνειας του GDPR.

Ένα άλλο πολύ σοβαρό σχόλιο είναι ότι στην πολιτική απορρήτου της Mi Fit αναφέρεται ότι εάν ο χρήστης κοινοποιήσει τα δεδομένα του σε άλλα άτομα, η εφαρμογή θα συλλέξει δεδομένα από τα άλλα άτομα χωρίς της γνώση ή την συγκατάθεση αυτών. Αυτό όμως, όπως είναι διατυπωμένο, παραπέμπει, ως επεξεργασία, στην περίπτωση της Cambridge Analytica, που εφόσον γίνεται αυτό είναι πολύ σοβαρό και σίγουρα θα επιφέρει μεγάλο πρόστιμο στην εταιρία.

Ένα άλλο σημείο στην ίδια πολιτική απορρήτου είναι το σημείο όπου αναφέρει ότι εάν ο χρήστης ανακαλέσει την συγκατάθεση του για παροχή των προσωπικών του δεδομένων η εταιρία μπορεί να του απαγορεύσει την χρήση των υπηρεσιών της. Αυτό όμως, κατ' αρχήν, εναντιώνεται στην ελεύθερη παροχή της συγκατάθεσης και με τον τρόπο της η εταιρία

εξαναγκάζει τον χρήστη να δώσει την συγκατάθεσή του και να μην την ανακαλέσει αλλιώς θα έχει επιπτώσεις.

Κεφάλαιο 5

Αξιολόγηση

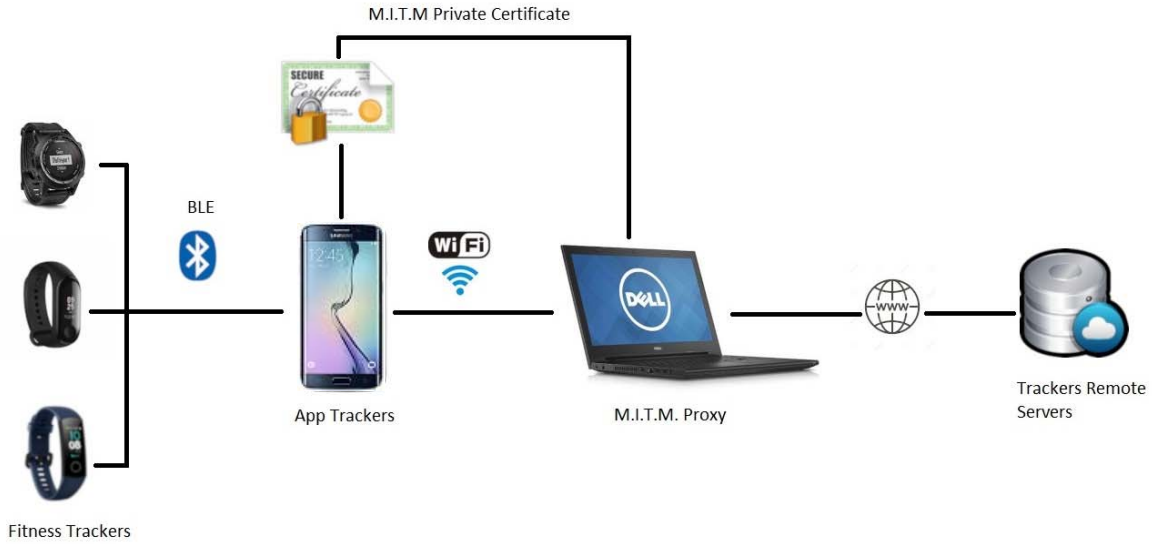
5.1 Γενικά

Στο παρόν κεφάλαιο περιγράφεται η πειραματική διαδικασία που ακολουθήθηκε, προκειμένου να αποτιμηθούν οι εφαρμογές μέτρησης φυσικής κατάστασης ως προς την επεξεργασία προσωπικών δεδομένων που πραγματοποιούν.

5.2 Πειραματική Διάταξη

Στην πειραματική διάταξη, όπως φαίνεται στην εικόνα 2, συνδέθηκαν οι fitness trackers που θα εξεταστούν σε αυτή την μελέτη, μέσω πρωτοκόλλου Bluetooth, σε ένα Samsung Galaxy S6 Edge (SM-G925F), το οποίο τρέχει λειτουργικό Android 7.0. Εδώ πρέπει να σημειωθεί ότι η Google από το Android 7 (Nougat) και αργότερα δεν επιτρέπει την εγκατάσταση private certificates από τρίτους[18], που θα χρειαστεί αργότερα. Για την πειραματική διάταξη επειδή ήταν απαραίτητη η εγκατάσταση ενός τέτοιου certificate, χρειάστηκε να γίνει το κινητό root μέσω του προγράμματος Magisk[19] και μέσω της μεθοδολογίας (Github 2015) τα certificate’s που δημιουργήθηκαν για αυτό τον σκοπό πλέον αναγνωρίζονται ως system certificates. Επίσης πάνω την συσκευή εγκαταστάθηκαν όλες οι εφαρμογές των πιο πάνω fitness trackers, όπως και οι εφαρμογές που θα χρησιμοποιούν το ίδιο το smartphone για συλλογή δεδομένων μέσω του επίσημου Play Store.

[18] https://android-developers.googleblog.com/2016/07/changes-to-trusted-certificate.html
[19] https://magiskmanager.com/



Εικόνα 2. Αναπαράσταση της πειραματικής διάταξης.

Παράλληλα εγκαταστάθηκε το Lumen Privacy Monitor[20] το οποίο είναι ένα δωρεάν ειδικό λογισμικό το οποίο αναλύει διεξοδικά όλο το εξερχόμενο traffic του κινητού στο κομμάτι της προστασίας προσωπικών δεδομένων. Το εργαλείο αυτό έχει αξιοποιηθεί από πολλούς ερευνητές για την ανάλυση της εξερχόμενης κίνησης από «έξυπνες» εφαρμογές. Το Lumen λειτουργεί στην συσκευή ως ένας μεσάζων κατά την διαδικασία αποστολής δεδομένων από την συσκευή σε τρίτους, «υποκλέπτοντας» και αναλύοντας όλο το εξερχόμενο traffic, ακριβώς με στόχο τη διερεύνηση του κατά πόσον μία εφαρμογή πλήττει την ιδιωτικότητα του χρήστη. Έχει την δυνατότητα αυτόματης εγκατάστασης ενός TLS Certificate το οποίο θα χρησιμοποιηθεί έτσι ώστε να μπορούν να αναλυθούν και τα δεδομένα που εξέρχονται μέσω πρωτοκόλλου TLS.

Εκτός από το Lumen χρησιμοποιήθηκε και το λογισμικό ανοικτού κώδικα του OWASP Zed Attack Proxy (ZAP) v2.7 [21] όπως και το δωρεάν λογισμικό Burp Suite Community Edition v1.7.36 [22] τα οποία εγκαταστάθηκαν στο Dell Inspiron Laptop της πειραματικής διάταξης σε λειτουργικό σύστημα Windows 10. Επίσης δημιουργήθηκαν άλλα δυο certificates (ένα για το κάθε λογισμικό) τα οποία εγκαταστάθηκαν στο smartphone με την διαδικασία (Github 2015). Αφού έχουν εγκατασταθεί τα δυο αυτά certificate έγιναν δυο ξεχωριστά HTTP(S) Proxy's, μεταξύ της Android συσκευής και των τελικών servers, επιτυγχάνοντας δηλαδή ένα

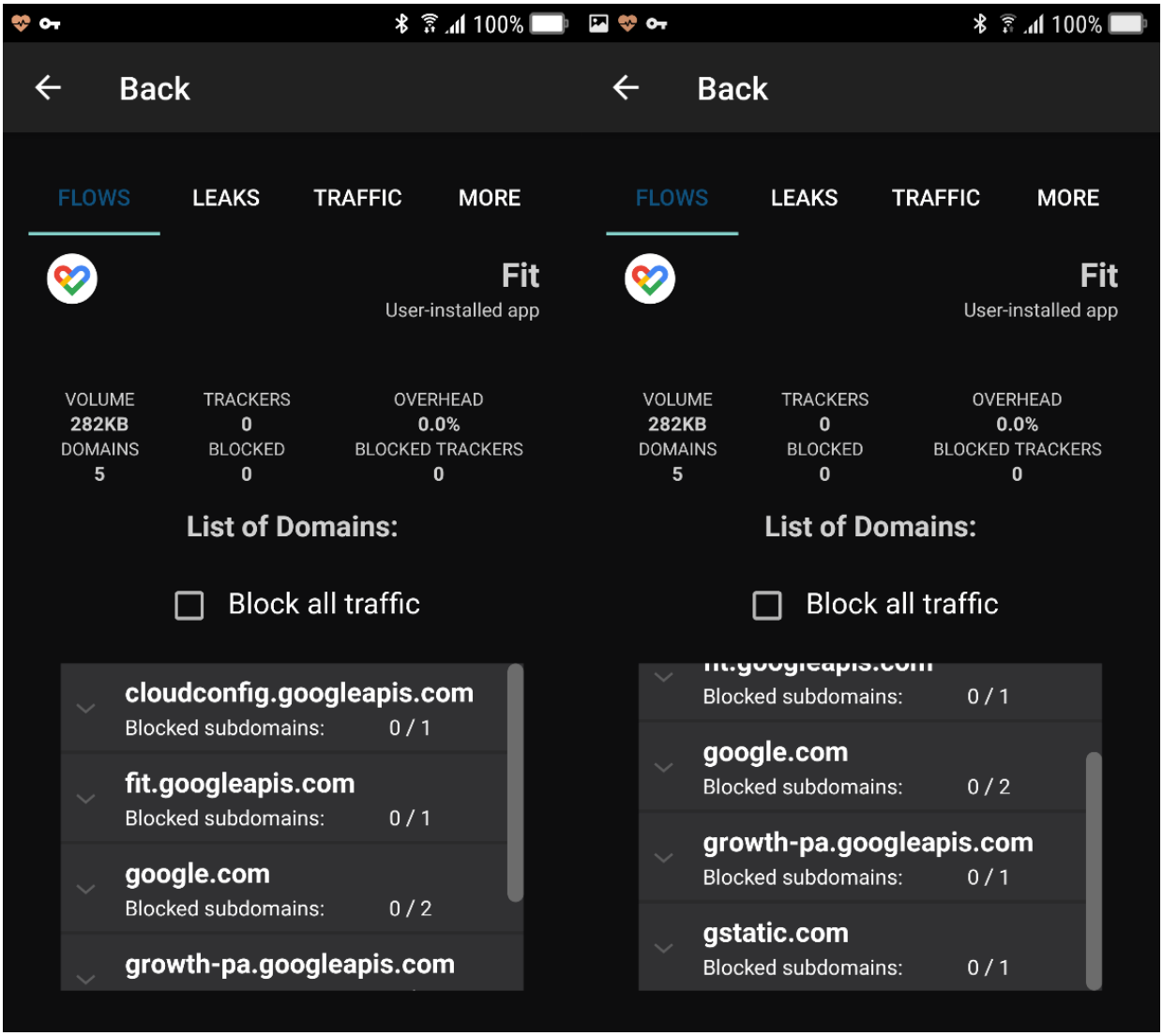
[20] https://www.haystack.mobi/
[21] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
[22] https://portswigger.net/burp/communitydownload

περιβάλλον Man In The Middle (M.I.T.M.). Σκοπός αυτής της διαρρύθμισης είναι να φιλτράρεται όλο το εξερχόμενο traffic από την συσκευή στο αντίστοιχο λογισμικό και να γίνεται ανάλυση αυτών των δεδομένων. Εδώ θα πρέπει να τονιστεί ότι λόγω της συγκεκριμένης μεθοδολογίας και τον τρόπο λειτουργίας των proxy, δεν είναι δυνατό η ταυτόχρονη λειτουργία όλων αυτών των εφαρμογών. Έτσι έπρεπε κάθε φορά να εξετάζει όλο το εξερχόμενο traffic μια εφαρμογή την φορά, που όπως θα διαφανεί και αργότερα, είναι αδύνατον όλα αυτά τα δεδομένα να είναι ακριβώς τα ίδια, γι' αυτό και κάθε εφαρμογή θα παρουσιάζει διαφορετικά αποτελέσματα, όχι όμως ικανά για να αλλάξουν την αξιολόγηση της κάθε εφαρμογής ως προς το σκέλος της συλλογής και αποστολής προσωπικών δεδομένων σε τρίτους.

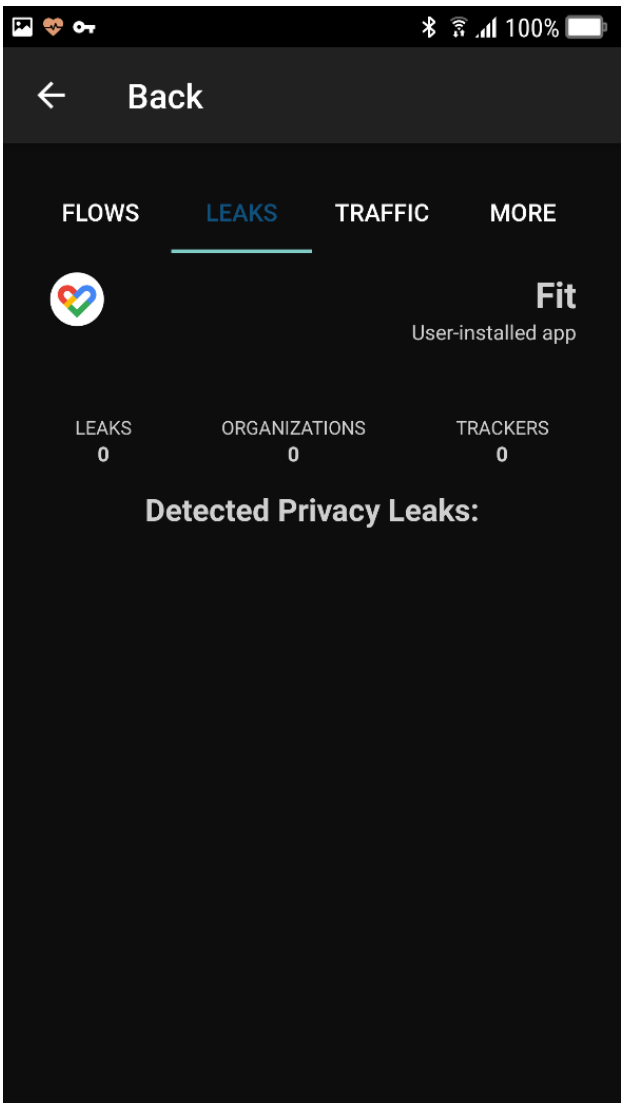
5.3 Ανάλυση των εφαρμογών

Αφού είχε εφαρμοστεί η πιο πάνω διάταξη, ξεκίνησε η τροφοδότηση δεδομένων σε όλες τις εξεταζόμενες συσκευές. Αυτό επιτεύχθηκε μέσω της καθημερινής χρήσης των εν λόγω συσκευών στην καθημερινή μου ζωή. Για την καλύτερη ανάλυση του traffic των δεδομένων των εφαρμογών, το smartphone (Samsung Galaxy S6), δεν συνδεόταν με το διαδίκτυο παρά μόνο όταν θα έμπαινε στο περιβάλλον M.I.T.M., έτσι ώστε όλο το εξερχόμενο traffic να φιλτράρεται από τις πιο πάνω εφαρμογές. Η περίοδος που διεξήχθησαν οι πιο πάνω μετρήσεις ήταν από τις 11 Απρ 2019 μέχρι τις 17 Οκτ 2019.

5.3.1 Google Fit

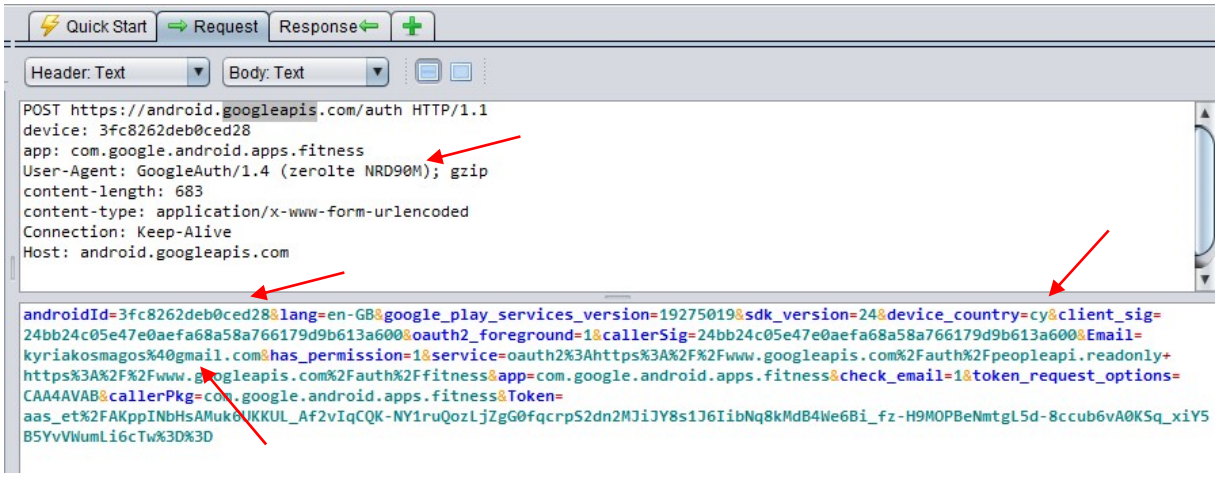


Εικόνα 3. Lumen - παρουσιάζονται όλες οι ροές της εφαρμογής Google Fit προς όλους τους servers.

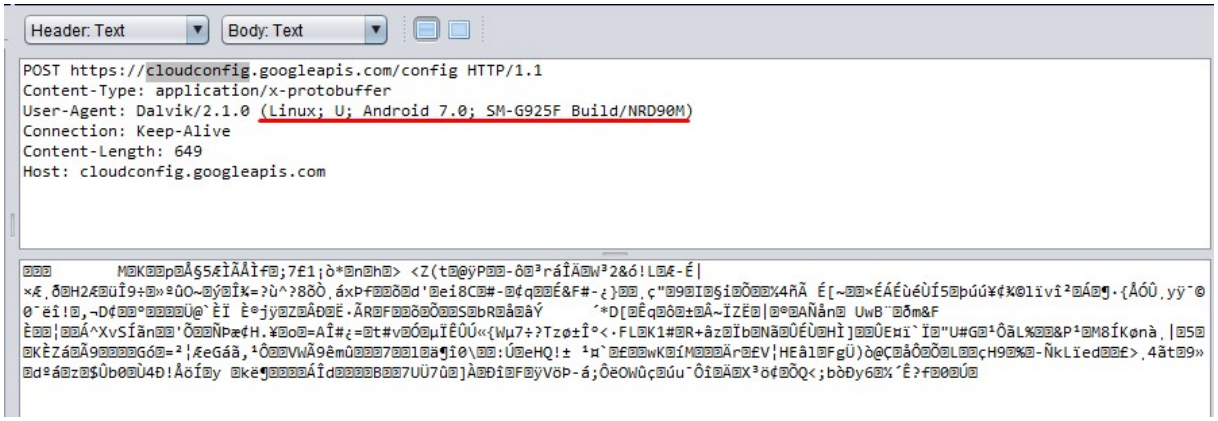


Εικόνα 4. Lumen - δεν βρέθηκαν διαρροές προσωπικών δεδομένων.

Όπως παρουσιάζει το Lumen, η εφαρμογή του Google Fit στέλνει τα δεδομένα από την συσκευή σε 5 domains (cloudconfig.googleapis.com, fit.googleapis.com, clients4.google.com, growth-pa.googleapis.com, csi.gstatic.com), ενώ στην συνέχεια δεν βρίσκει καθόλου διαρροές προσωπικών δεδομένων σε τρίτους. Όλα τα πιο πάνω domains ανήκουν στην Google.

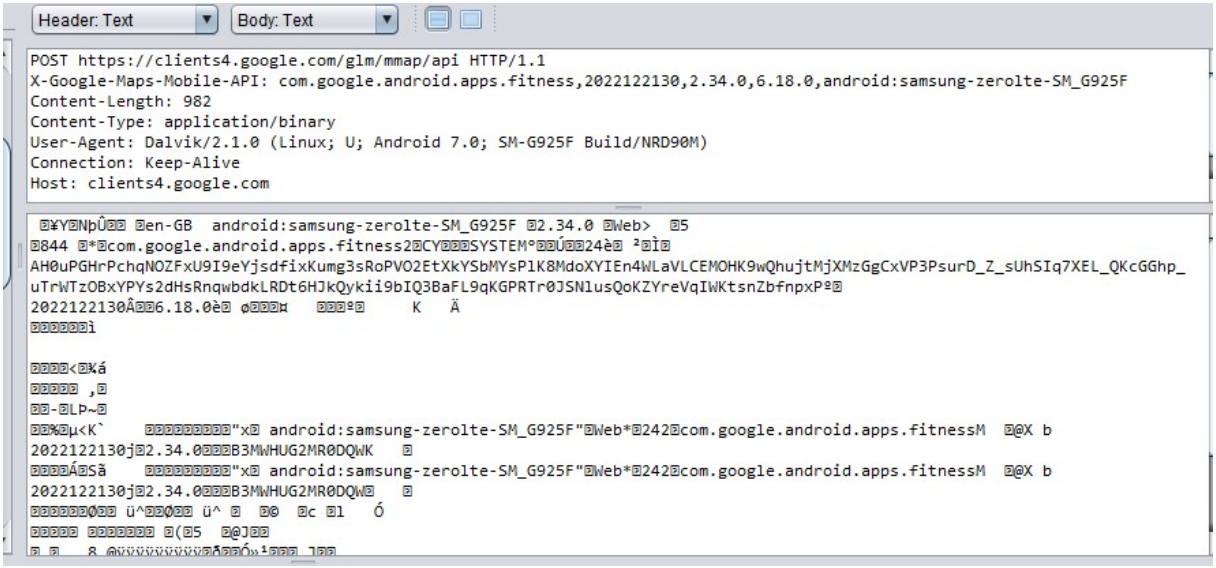


Εικόνα 5. OWASP ZAP - παρατηρείται ότι αποστέλλονται δεδομένα όπως το GAID (Google Advertising ID), χώρα, email, όπως επίσης και το build fingerprint.



Εικόνα 6. OWASP ZAP - παρατηρείται ότι αποστέλλονται δεδομένα όπως το μοντέλο της συσκευής και το build fingerprint.

Στην αξιολόγηση με το OWASP ZAP, αφού έχει γίνει ανάλυση, παρατηρήθηκαν να αποστέλλονται δεδομένα προσωπικού χαρακτήρα όπως το GAID, χώρα του χρήστη, το email, και το build fingerprint. Εδώ θα πρέπει να τονιστεί ότι αυτά τα δεδομένα αποστέλλονται στα πιο πάνω domain μέσω πρωτοκόλλου TLS, δηλαδή υπό κανονικές συνθήκες αυτά θα παρουσιάζονταν κρυπτογραφημένα. Ωστόσο στην Εικόνα 6 και 7 παρουσιάζονται κρυπτογραφημένα δεδομένα που σημαίνει ότι η εφαρμογή κρυπτογραφεί τα δεδομένα πριν από το επίπεδο της μεταφοράς για περισσότερη προστασία των δεδομένων αυτής. Ακόμα και σε αυτή την πειραματική διάταξη, η ανάλυση αυτών των εξερχομένων δεδομένων κρίνεται αδύνατη.

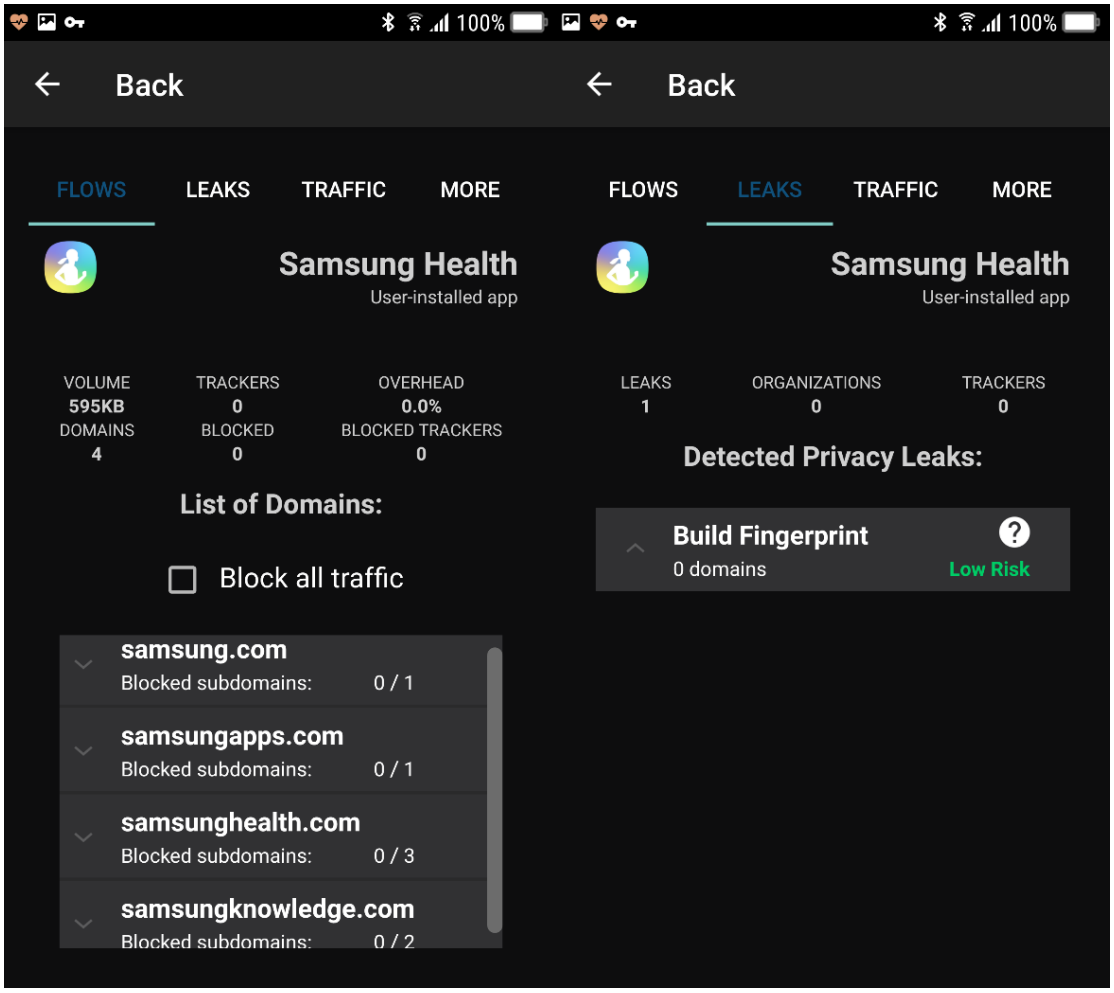


Εικόνα 7. OWASP ZAP – Κρυπτογραφημένα δεδομένα που αποστέλλονται μέσω του Google API.

	cloudconfig.googleapis.com	fit.googleapis.com	clients4.google.com	growth-pa.googleapis.com	android.googleapis.com	csi.gstatic.com
Build Fingerprint	✓		✓		✓	
Όνομα Συσκευής	✓		✓		✓	
GAID					✓	
Χώρα					✓	
email					✓	
Κρυπτογραφημένα	✓		✓			

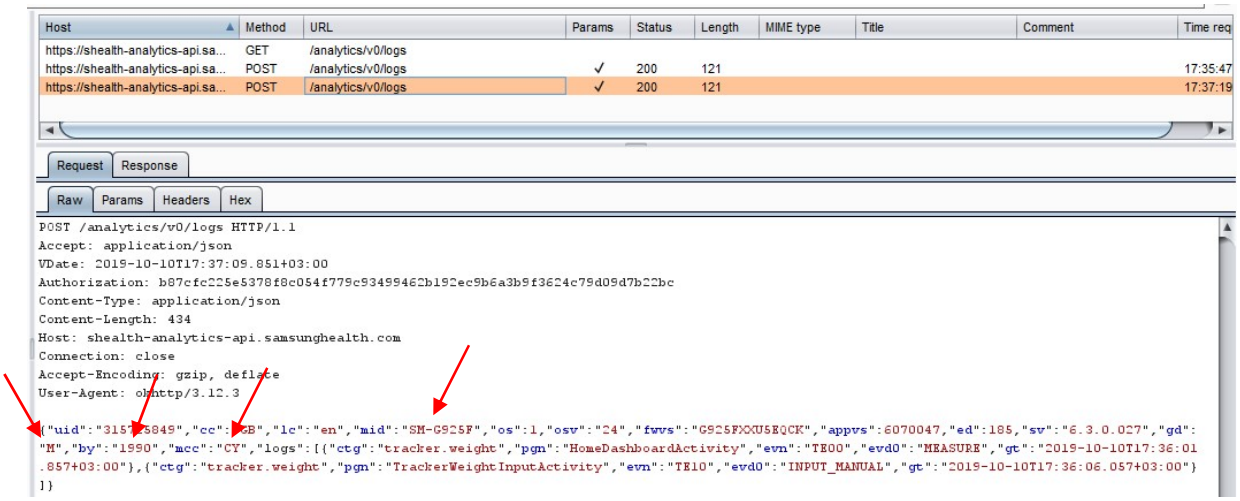
Πίνακας 2. Παρουσίαση δεδομένων προσωπικού χαρακτήρα που βρέθηκαν να συλλέγονται ανά domain στην εφαρμογή Google Fit.

5.3.2 Samsung Health

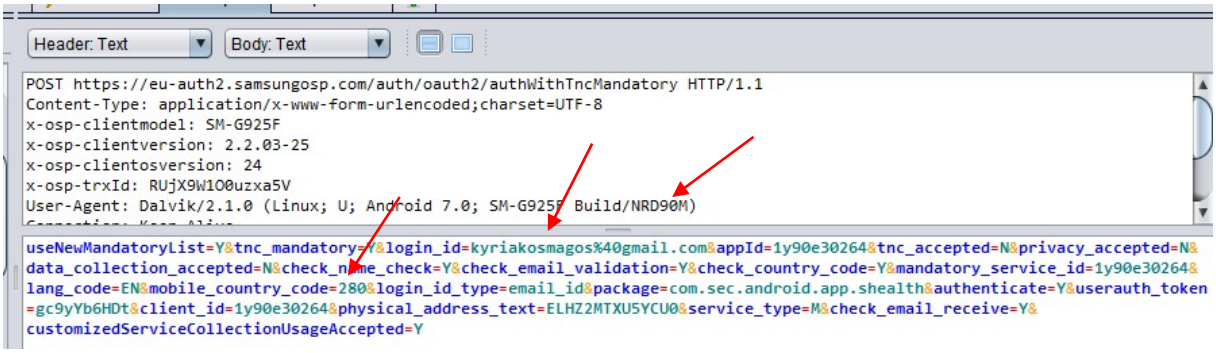


Εικόνα 8. Lumen - Παρουσιάζονται όλες οι ροές της εφαρμογής Samsung Health προς όλους τους servers όπως επίσης και μη διαρροή προσωπικών δεδομένων.

Η ανάλυση του Lumen, για την εφαρμογή Samsung Health δείχνει ότι στέλνει τα δεδομένα από την συσκευή σε 4 domains (dls.di.atlas.samsung.com, vas.samsungapps.com, samsunghealth.com, samsungknowledge.com), ενώ πάλι στην συνέχεια δεν βρίσκει καθόλου διαρροές προσωπικών δεδομένων σε τρίτους. Όλα τα πιο πάνω domains ανήκουν στην Samsung.

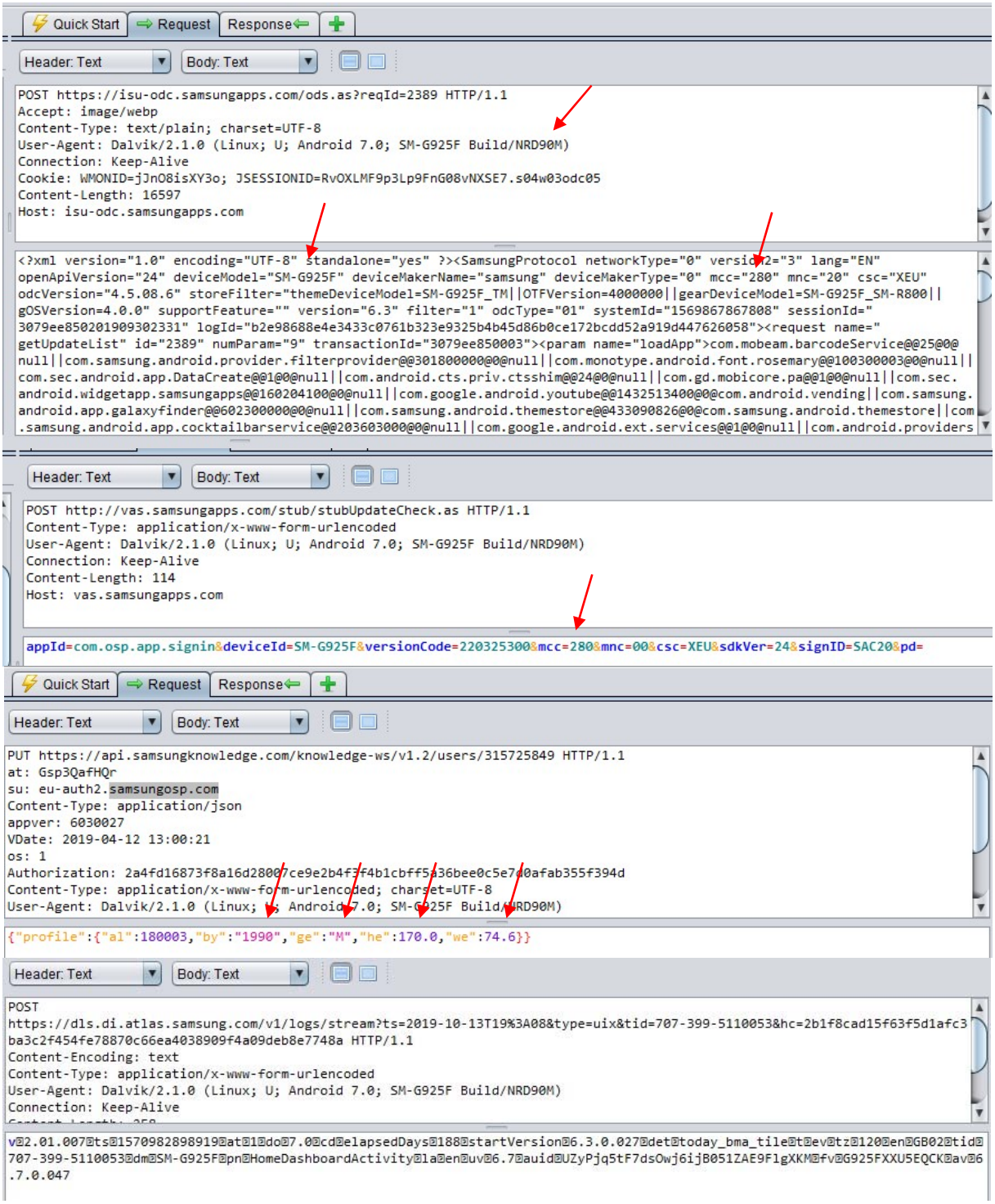


Εικόνα 9. Burp Suite - παρατηρείται ότι αποστέλλονται δεδομένα όπως το μοντέλο της συσκευής, το φύλο, το έτος γέννησης και η χώρα του χρήστη.



Εικόνα 10. OWASP ZAP - παρατηρείται ότι αποστέλλονται δεδομένα όπως το μοντέλο της συσκευής, το build fingerprint, το email και η χώρα του χρήστη.

Ακολούθως στην ανάλυση μέσω του Burp Suite (Εικόνα 9) και OWASP ZAP (Εικόνα 10) παρατηρείται ότι αποστέλλονται δεδομένα προσωπικού χαρακτήρα όπως το μοντέλο της συσκευής, το build fingerprint, το φύλο, το έτος γέννησης, το email και η χώρα του χρήστη.



Εικόνα 11. OWASP ZAP – Διάφορες ροές δεδομένων προς domains της Samsung.

Εικόνα 12. OWASP ZAP – Ροή δεδομένων προς domain της Google.

Όπως έχει παρατηρηθεί και στο Google Fit, όλες οι δραστηριότητες του χρήστη στέλνονται στον συγκεκριμένο library της Google (Εικόνα 12) με μια μορφή κρυπτογράφησης. Δεν έχει παρατηρηθεί οποιαδήποτε δραστηριότητα του χρήστη να στέλνεται προς libraries της Samsung εκτός αυτό εάν γίνεται με ψεδονυμωποίηση και δεν μπορεί να καθοριστεί από τις ροές που αναλύθηκαν, λόγω άγνωστης τιμής που ενδέχεται να παίρνουν οι μεταβλητές της κάθε δραστηριότητας.

Εικόνα 13. OWASP ZAP – Ροή δεδομένων προς domain τρίτου.

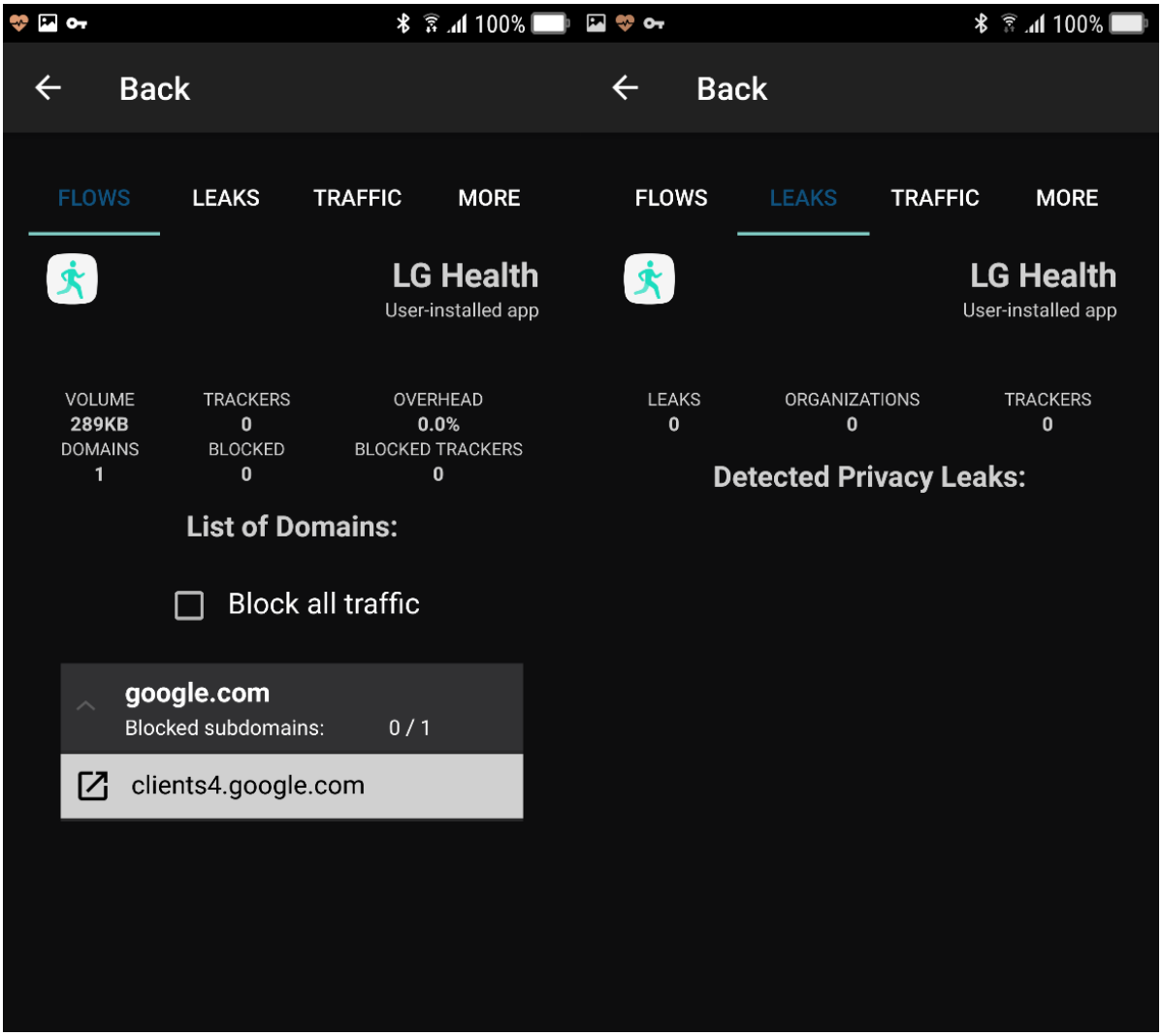
Όπως φαίνεται στην Εικόνα 13, έχει καταγραφεί από τον χρήστη ότι έφαγε αυγό για δείπνο. Η εφαρμογή φαίνεται ότι για το κομμάτι της διατροφής συνεργάζεται με την εταιρία Fatsecret[23] της οποίας χρησιμοποιεί την πλατφόρμα της για την καταγραφή και μέτρηση γευμάτων και θερμίδων των χρηστών της.

[23] https://platform.fatsecret.com/

	dls.di.atlas.samsung.com	vas.samsungapps.com	samsunghealth.com	samsungknowledge.com	clients4.google.com	Fatsecret.com	eu-auth2.samsungosp.com	isu-odc.samsungapps.com
Build Fingerprint	✓	✓	✓	✓	✓	✓	✓	✓
Όνομα Συσκευής	✓	✓	✓	✓	✓	✓	✓	✓
GAID								
Χώρα		✓	✓				✓	✓
email			✓				✓	
Έτος Γέννησης			✓	✓				
Δεδομένα Υγείας και φυσικής κατάστασης			✓	✓				
Δεδομένα διατροφής						✓		
Κρυπτογραφημένα	✓				✓			

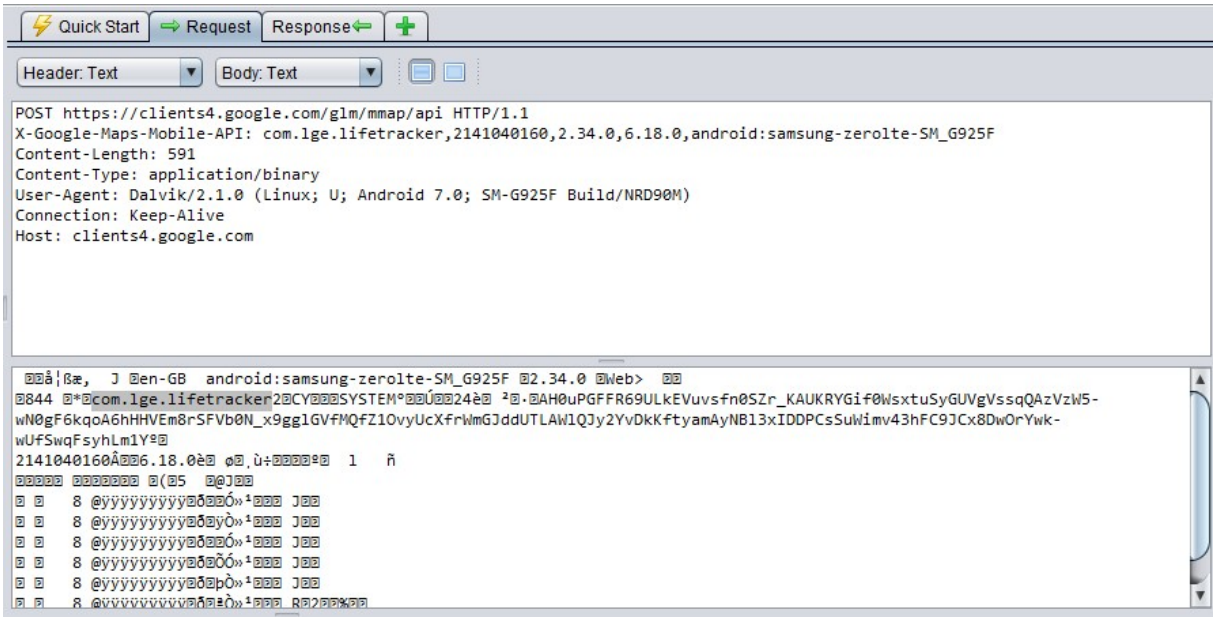
Πίνακας 3. Παρουσίαση δεδομένων προσωπικού χαρακτήρα που βρέθηκαν να συλλέγονται ανά domain στην εφαρμογή Samsung Health.

5.3.3 LG Health

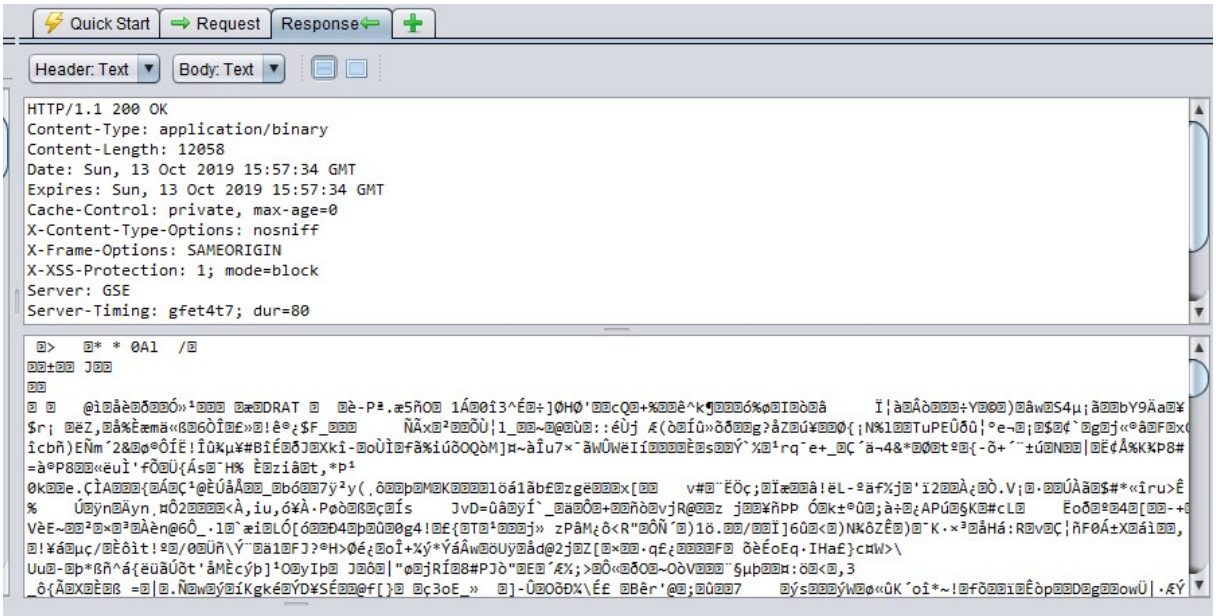


Εικόνα 14. Lumen - Παρουσιάζονται όλες οι ροές της εφαρμογής LG Health προς όλους τους servers όπως επίσης και μη διαρροή προσωπικών δεδομένων.

Η εφαρμογή της LG είναι η μόνη στις υπό αξιολόγηση εφαρμογές που δεν έχει ροές σε δικούς της servers παρά μόνο στην Google. Όπως θα παρουσιαστεί πιο κάτω η εφαρμογή χρησιμοποιεί την πλατφόρμα της Google για την επεξεργασία των δραστηριοτήτων του χρήστη. Όπως φαίνεται (Εικόνα 15 και Εικόνα 16) η εφαρμογή αποστέλλει κρυπτογραφημένα τις δραστηριότητες του χρήστη. Αυτό έχει παρατηρηθεί και στις υπόλοιπες εφαρμογές, πράγμα που σημαίνει ότι η κρυπτογράφηση πρέπει να γίνεται από κάποιο service της Google, και ο domain απαντά πίσω πάλι κρυπτογραφημένα, επεξεργασμένα τα δεδομένα για να παρουσιαστούν στον χρήστη μέσω της αντίστοιχης εφαρμογής.



Εικόνα 15. OWASP ZAP – Ροή δεδομένων προς domain της Google

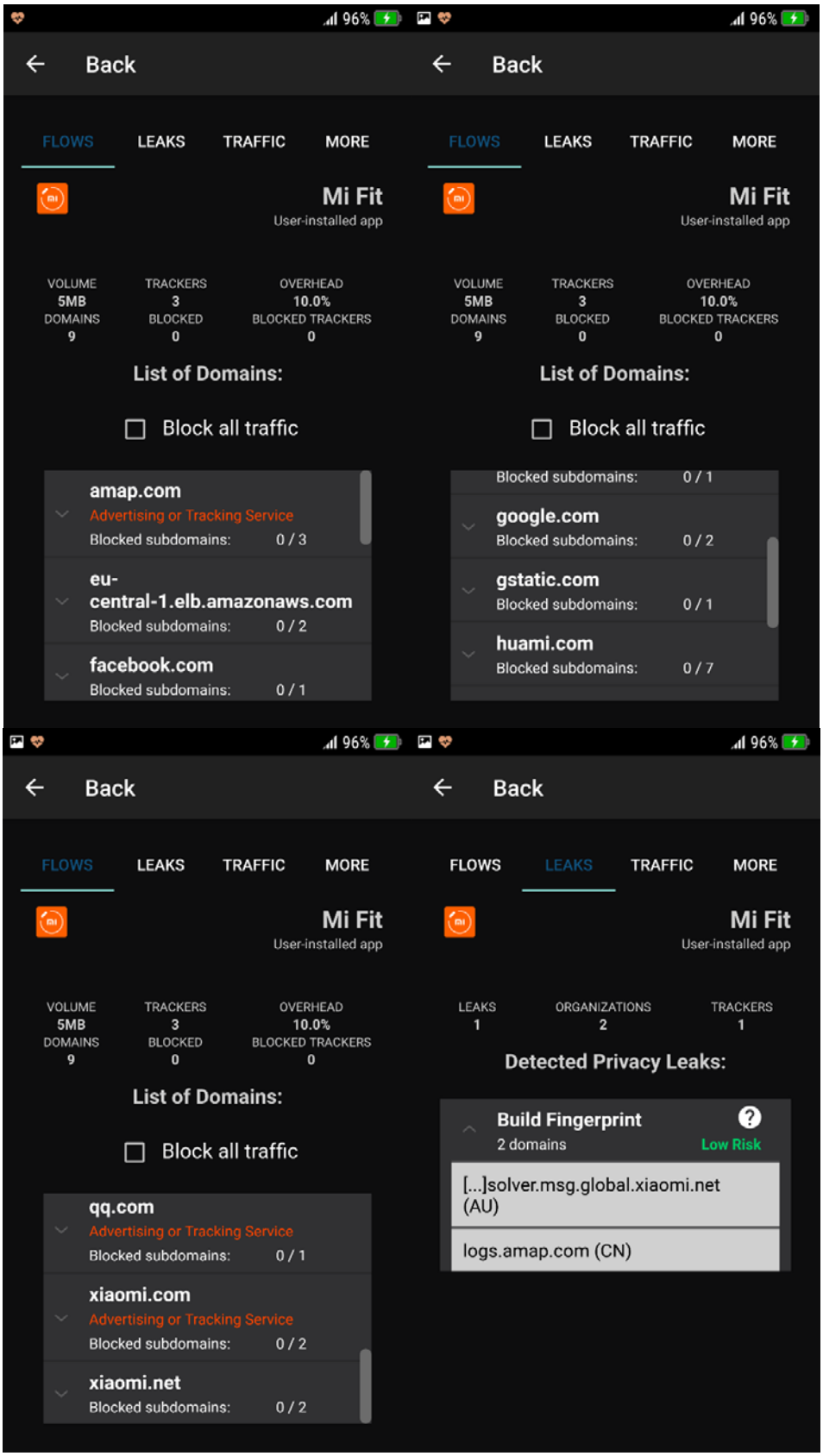


Εικόνα 16. OWASP ZAP – Απάντηση της προηγούμενης ροής από το domain της Google

	clients4.google.com
Build Fingerprint	✓
Όνομα Συσκευής	✓
GAID	
Χώρα	
email	
Κρυπτογραφημένα	✓

Πίνακας 4. Παρουσίαση δεδομένων προσωπικού χαρακτήρα που βρέθηκαν να συλλέγονται ανά domain στην εφαρμογή LG Health.

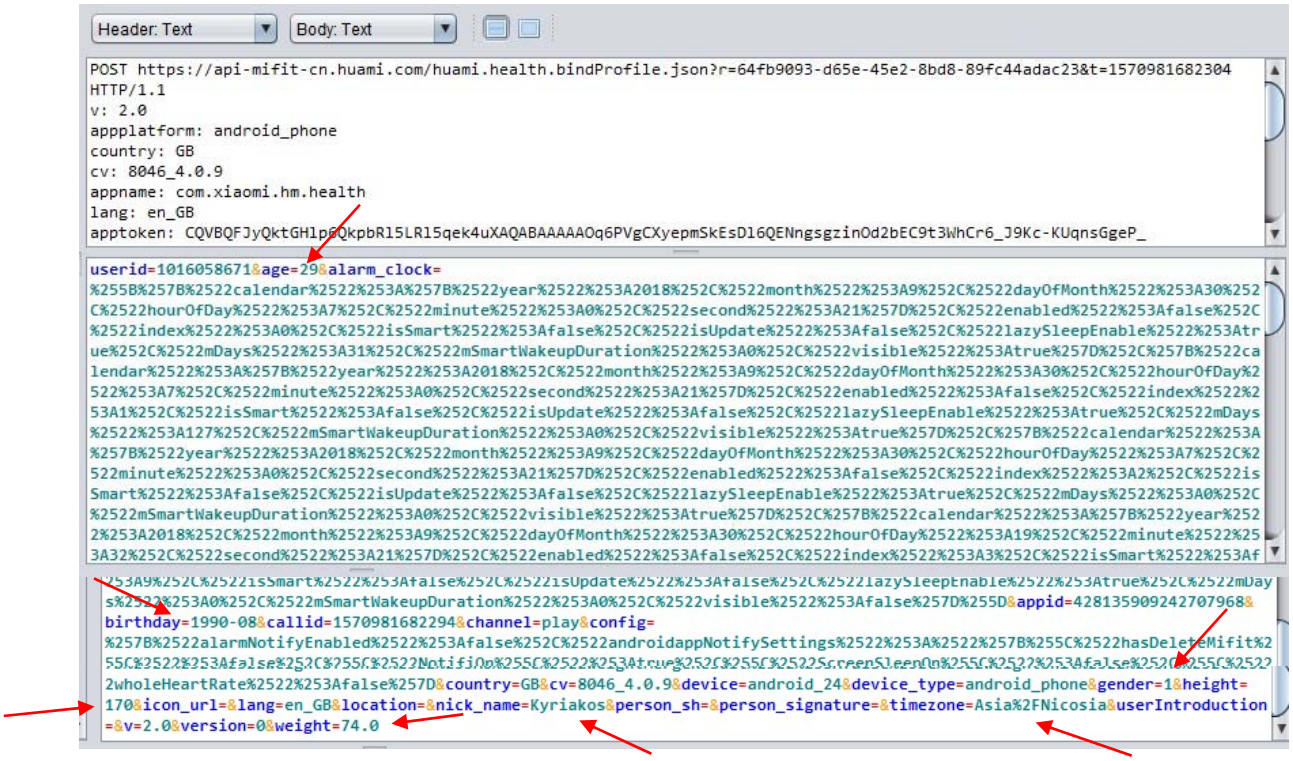
5.3.4 Mi Fit



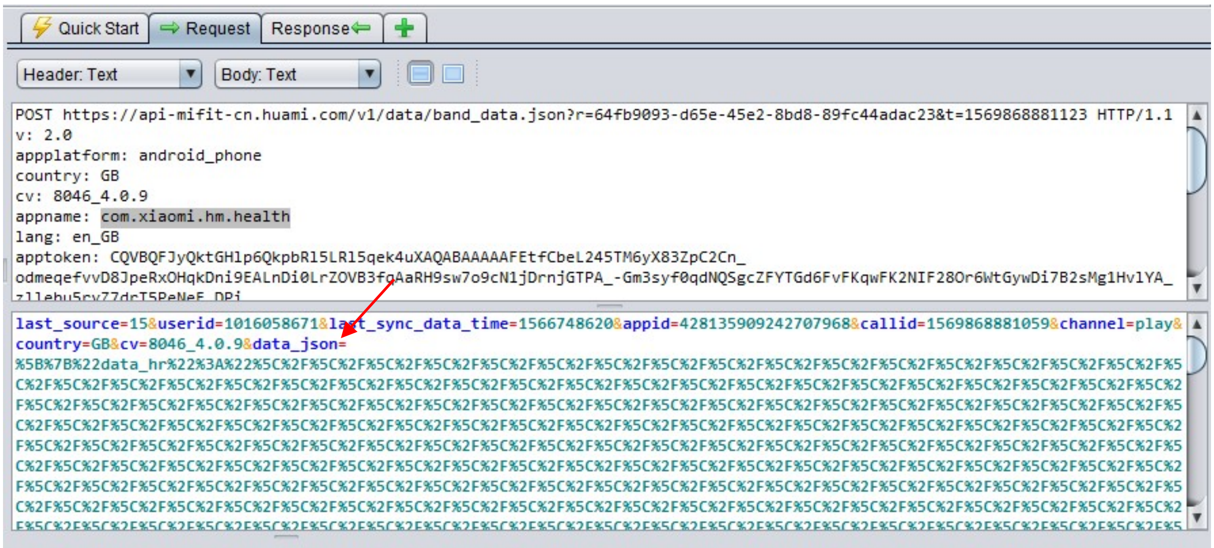
Εικόνα 17. Lumen - Παρουσιάζονται όλες οι ροές της εφαρμογής Mi Fit προς όλους τους servers όπως επίσης και διαρροή προσωπικών δεδομένων σε τρίτους.

Η ανάλυση του Lumen, για την εφαρμογή Mi Fit δείχνει ότι στέλνει τα δεδομένα από την συσκευή σε 9 domains (amap.com, eu-central-1.elb.amazonaws.com, graph.facebook.com, clients4google.com, cgi.gstatic.com, huami.com, cgi.connect.qq.com, xiaomi.com, xiaomi.net). Από όλα αυτά τα domains το Lumen χαρακτηρίζει το amap.com, cgi.connect.qq.com και το xiaomi.net ως διαφημιστικά ή κατασκοπευτικά. Δυστυχώς δεν μπορεί να δώσει με μεγαλύτερη ανάλυση κάτι περισσότερο οπότε θα γίνει καλύτερη ανάλυση με τις άλλες 2 εφαρμογές.

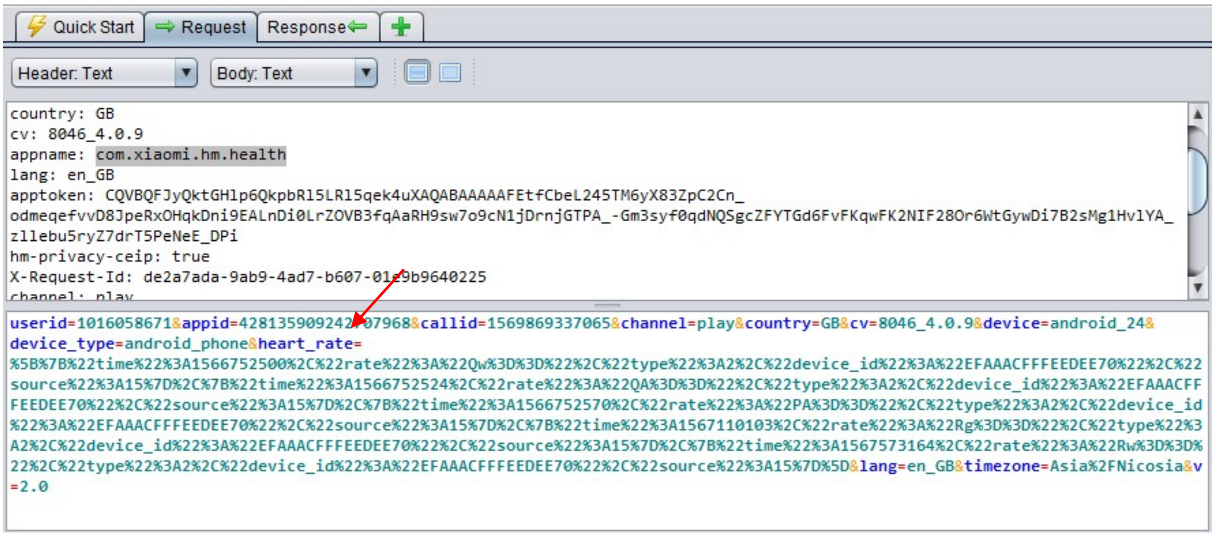
Όσον αφορά το κομμάτι των διαρροών δεδομένων το Lumen βρίσκει διαρροή του value build fingerprint στο domain resolver.msg.global.xiaomi.net και logs.amap.com.



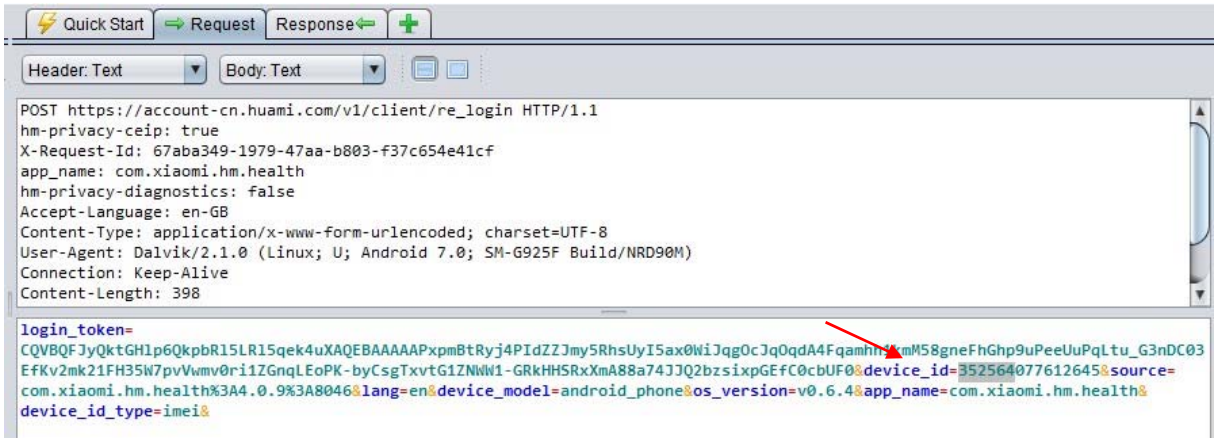
Εικόνα 18. OWASP ZAP - παρατηρείται ότι αποστέλλονται δεδομένα όπως το όνομα του χρήστη, τα γενέθλια - ηλικία, η ζώνη ώρας, το φύλο αλλά και ύψος και βάρος.



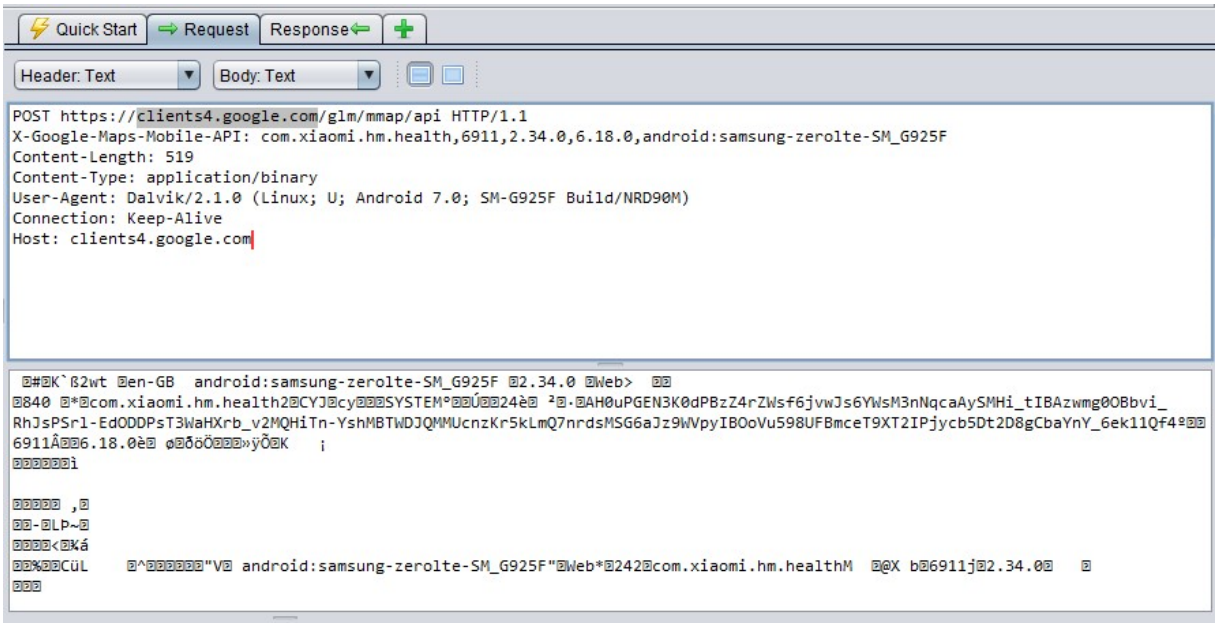
Εικόνα 19. OWASP ZAP – αυτά είναι δεδομένα που αποστέλλονται από την wearable συσκευή Mi Band 3 προς την εφαρμογή, και η εφαρμογή τα αποστέλλει στο library της.



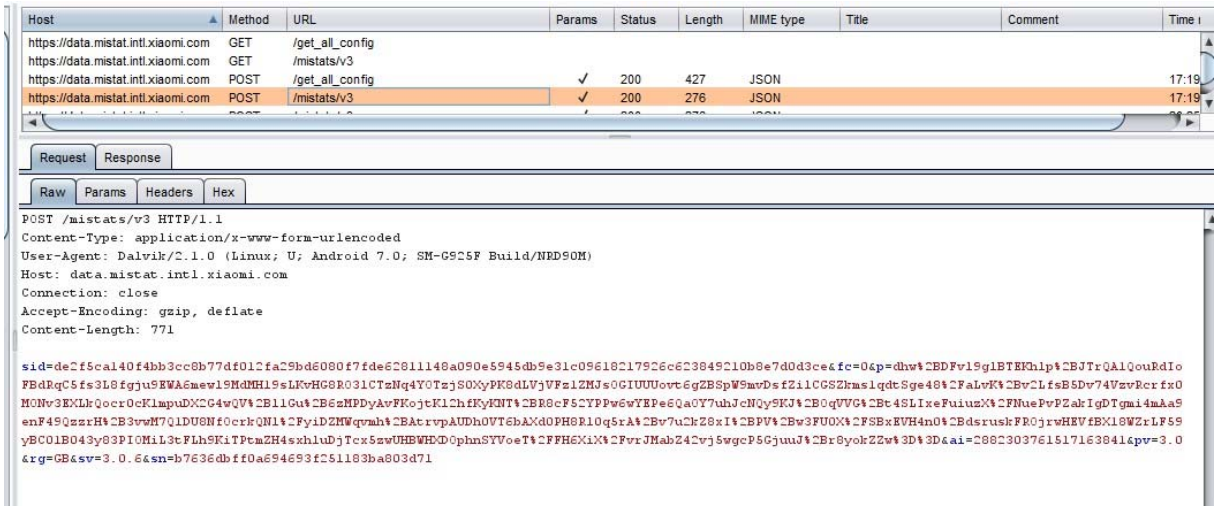
Εικόνα 20. OWASP ZAP – επιπρόσθετα δεδομένα που αποστέλλονται από την wearable συσκευή Mi Band 3 προς την εφαρμογή και αφορούν καρδιακούς παλμούς.



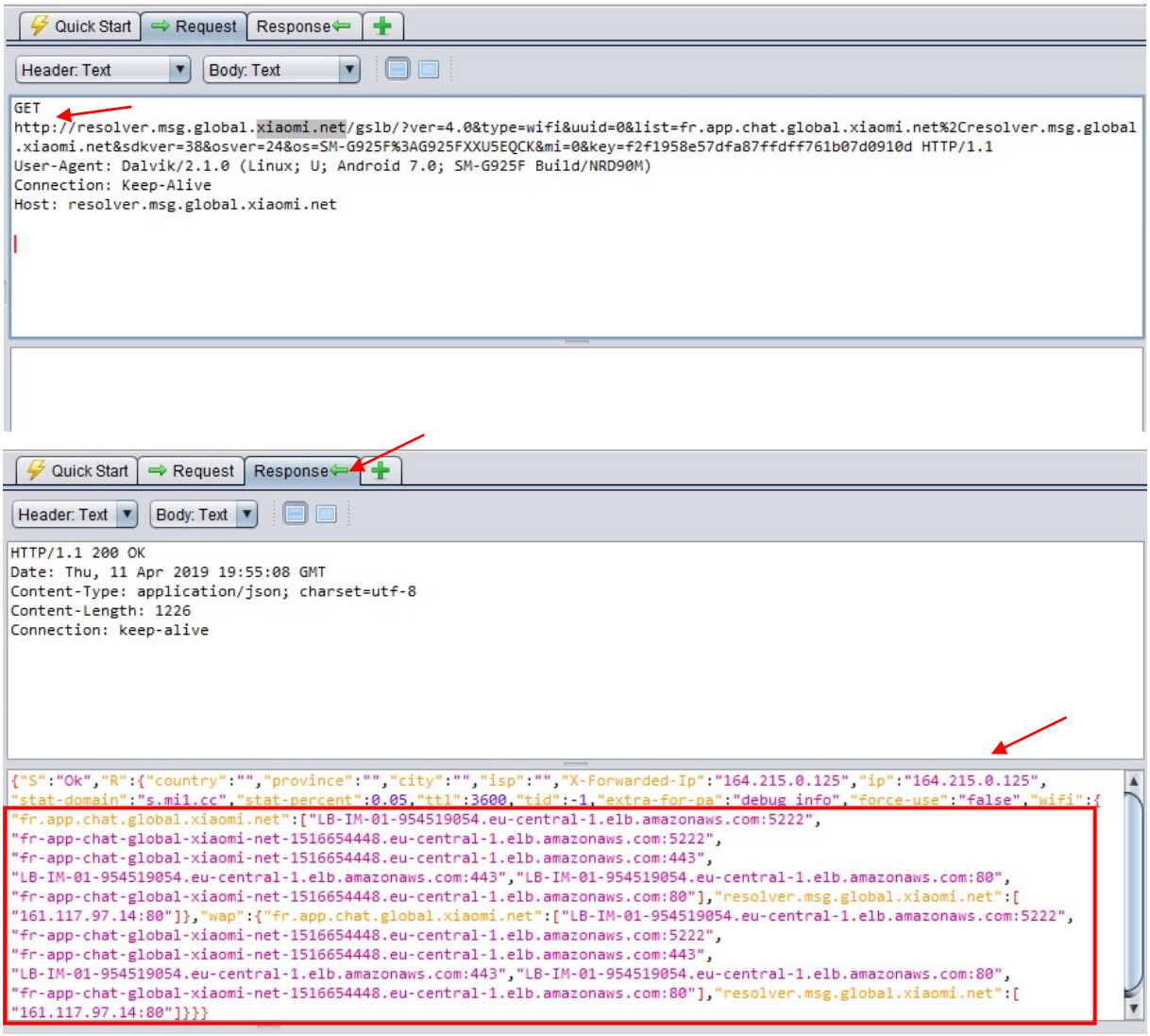
Εικόνα 21. OWASP ZAP – φαίνεται να ξαποστέλνει το IMEI της συσκευής για σκοπούς αυθεντικοποίησης.



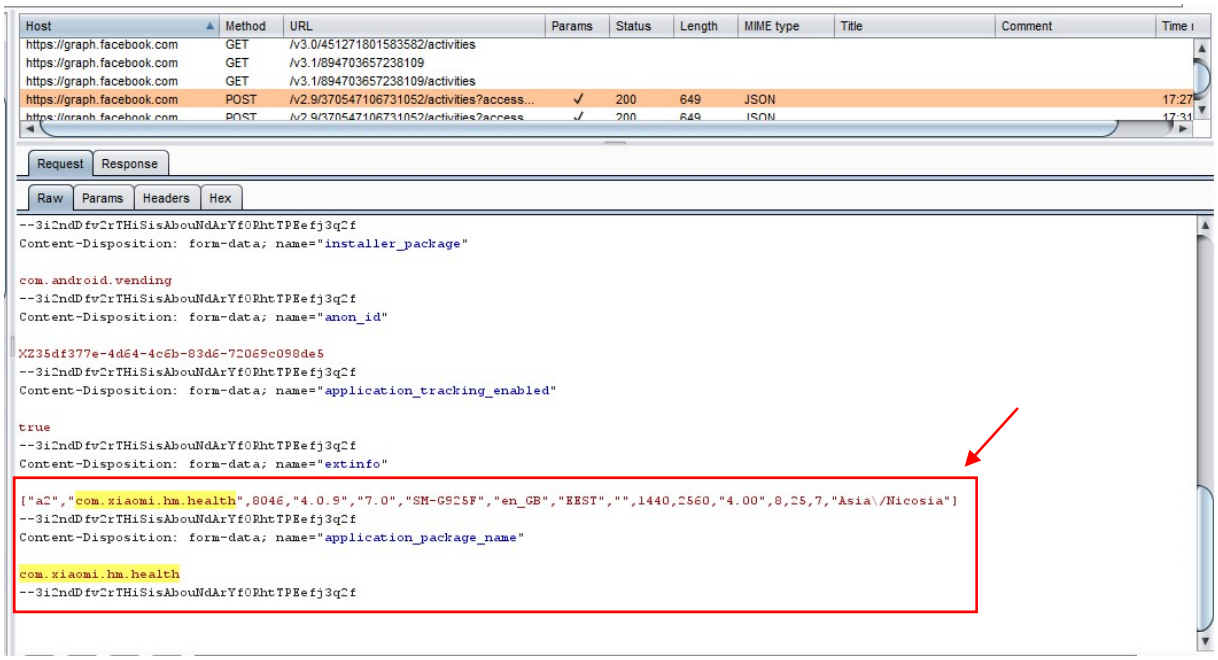
Εικόνα 22. OWASP ZAP – η Google για ακόμα μια φορά μέσω της πλατφόρμας της καταχωρεί και επεξεργάζεται κρυπτογραφημένα δεδομένα από την εφαρμογή Mi Health.



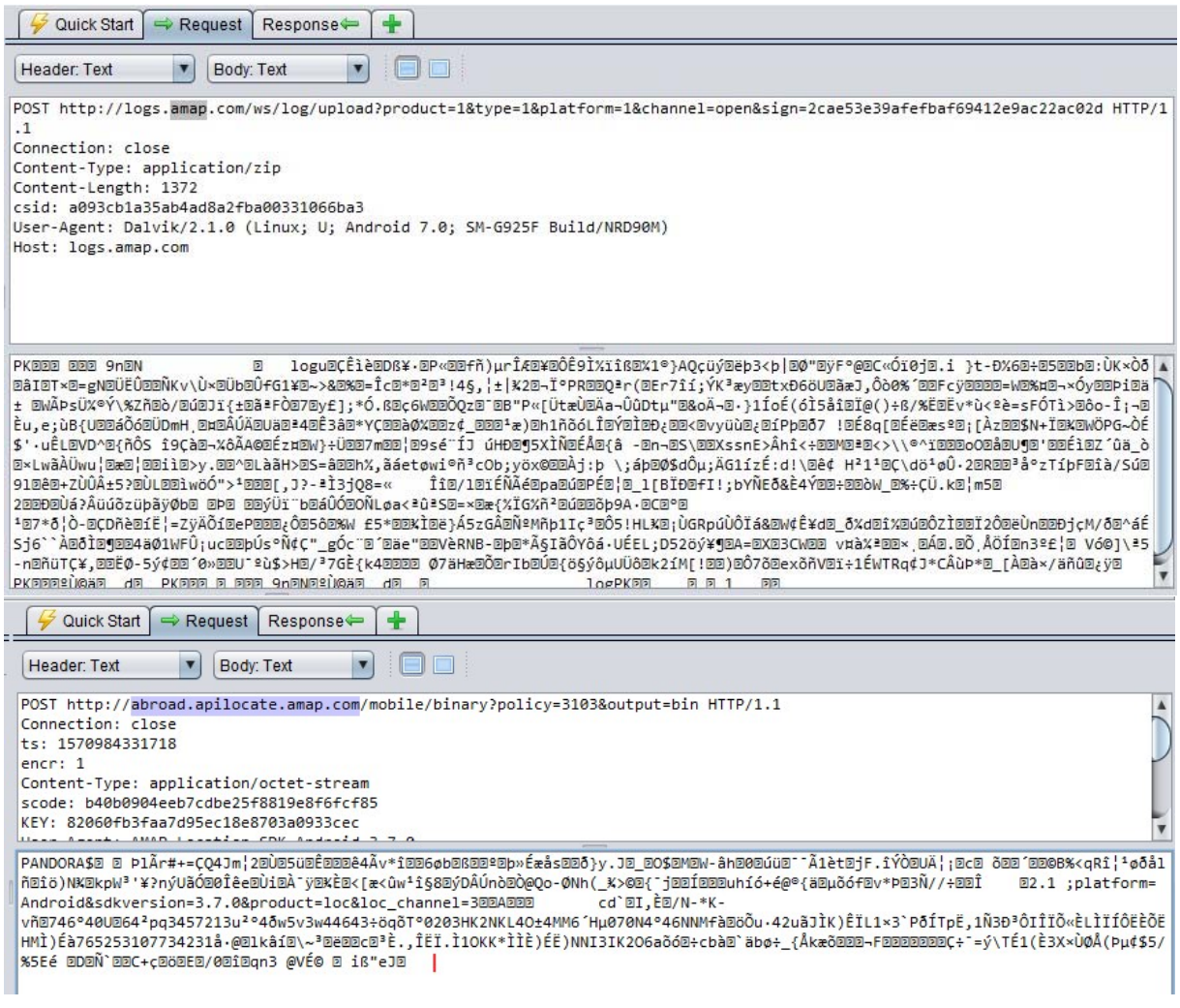
Εικόνα 23. Burp Suite – μια ροή προς το domain της xiaomi.com.



Εικόνα 24. OWASP ZAP – ροή προς το domain της xiaomi.net (που το Lumen ονόμαζε διαφημιστικό) δείχνει ότι ζητάει κάτι από το domain και αυτό απαντάει με άλλα domain που ανήκουν στην Amazon και επίσης περιλαμβάνει την IP διεύθυνση του χρήστη.

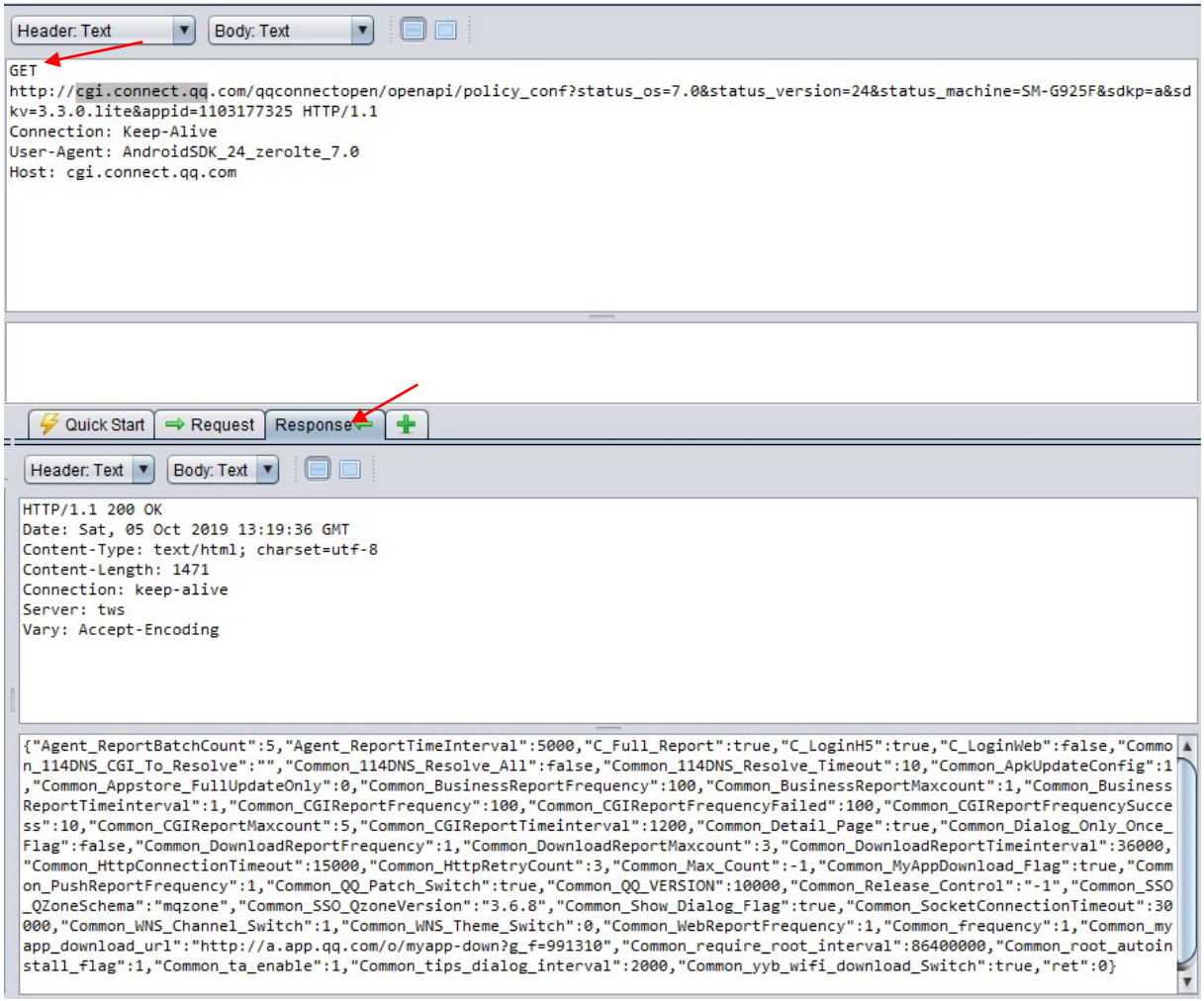


Εικόνα 25. Burp Suite – Αποστέλλονται στο facebook στοιχεία της συσκευής, όπως και το GAID



Εικόνα 26. OWASP ZAP – αποστολή κρυπτογραφημένων δεδομένων προς το domain amap.com.

Η πιο πάνω ροή δεδομένων είναι ίσως μια από τις πιο ανησυχητικές. Το domain amap.com ανήκει στην κινέζικη πολυεθνική εταιρία Alibaba η οποία είναι μια εταιρία κολοσσός της Κίνας με ειδίκευση το ηλεκτρονικό εμπόριο, cloud services κ.α. Όπως φαίνεται το περιεχόμενο της ροής είναι κρυπτογραφημένο με αποτέλεσμα να μην κατέστη εφικτό να διαφανεί τι δεδομένα αποστέλλονται στο domain.



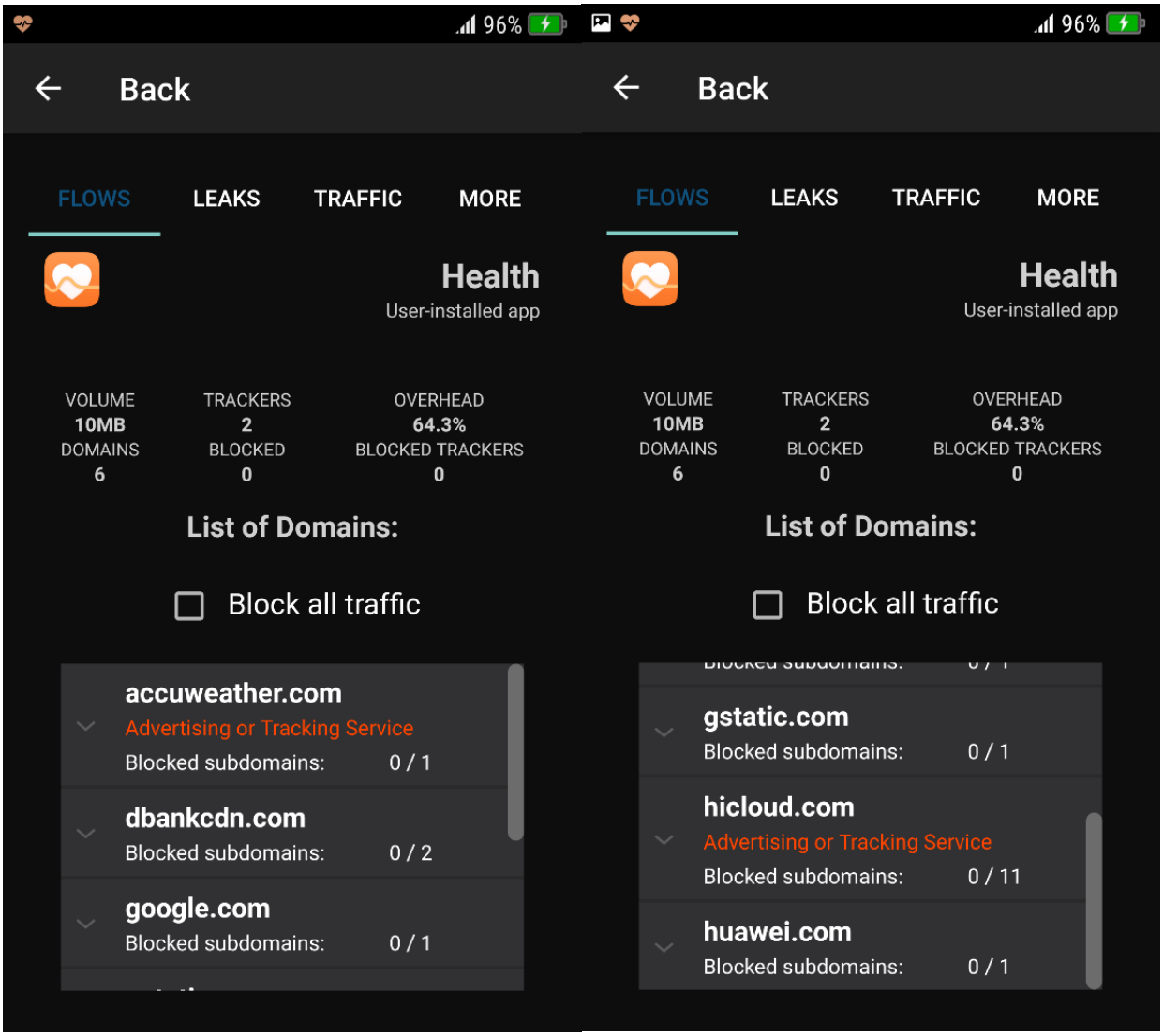
Εικόνα 27. OWASP ZAP – ροή προς το domain της qq.com (που το Lumen ονόμαζε διαφημιστικό) δείχνει ότι ζητάει κάτι από το domain και αυτό απαντάει.

Όπως και στην περίπτωση του amap.com και αυτό το domain ανήκει σε μια μεγάλη κινέζικη πολυεθνική εταιρία, την Shenzhen Tencent Computer Systems CO. Ltd η οποία ασχολείται κυρίως με υπηρεσίες στο διαδίκτυο. Ωστόσο από την ροή δεν φαίνεται να αποστέλλονται δεδομένα προσωπικού χαρακτήρα του χρήστη. Ενδεχομένως η εταιρία να προσφέρει κάποιο online service στην εφαρμογή του Mi Health.

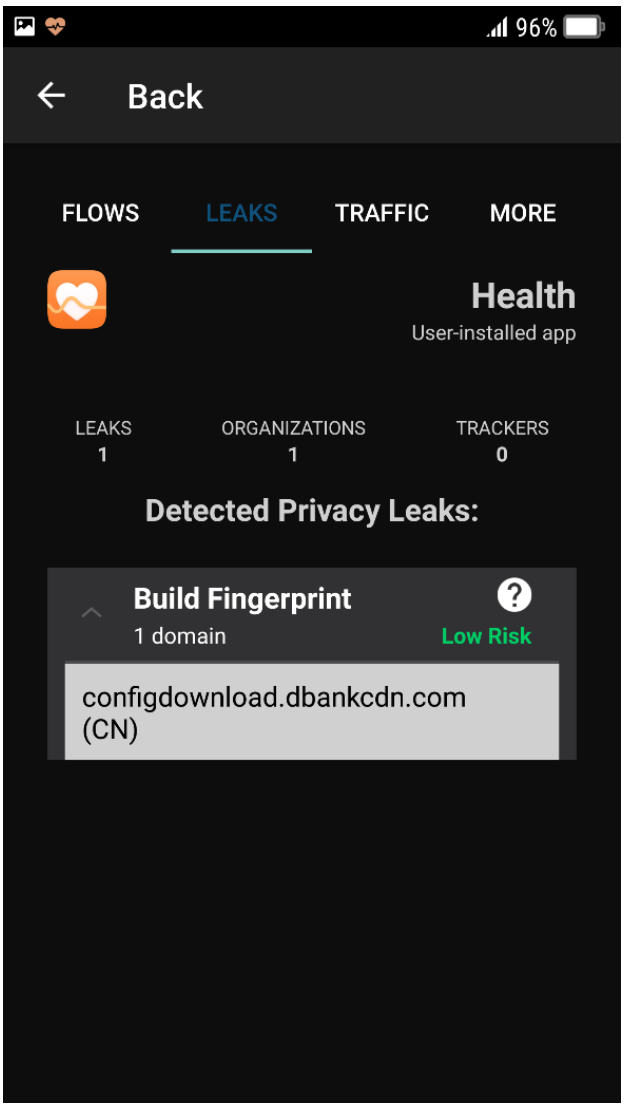
	amap.com	graph.facebook.com	clients4google.com	cgi.gstatic.com	huami.com	cgi.connect.qq.com	xiaomi.com	xiaomi.net
Build Fingerprint	✓	✓	✓		✓		✓	✓
Όνομα Συσκευής	✓	✓	✓		✓		✓	✓
GAID		✓						
IP Address								✓
IMEI					✓			
Ζώνη Ώρας					✓			
email								
Γενέθλια					✓			
Δεδομένα Υγείας και φυσικής κατάστασης					✓			
Δεδομένα Δραστηριότητας					✓			
Δεδομένα διατροφής								
Κρυπτογραφημένα	✓		✓					

Πίνακας 5. Παρουσίαση δεδομένων προσωπικού χαρακτήρα που βρέθηκαν να συλλέγονται ανά domain στην εφαρμογή Mi Fit.

5.3.5 Huawei Health



Εικόνα 28. Lumen - Παρουσιάζονται όλες οι ροές της εφαρμογής Health (Huawei) προς όλους τους servers.

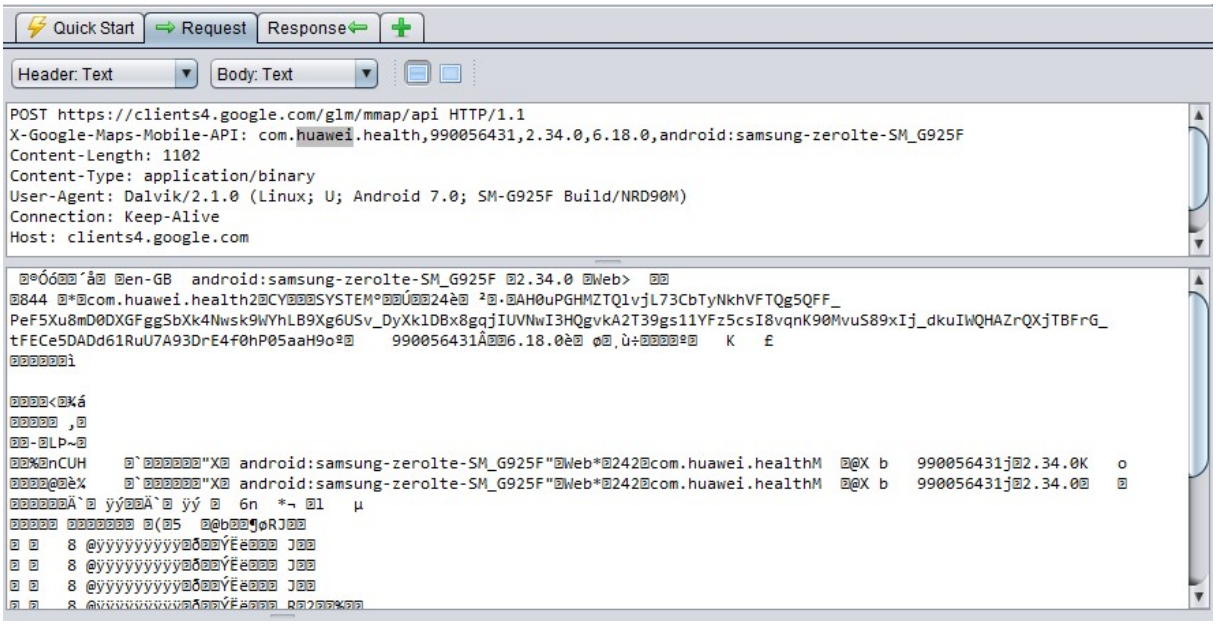


Εικόνα 29. Lumen – διαρροή του build Fingerprint σε domain

Η ανάλυση του Lumen, για την εφαρμογή Health (Huawei) είναι αρκετά ιδιάζουσα. Όπως δείχνει το Lumen, στέλνονται δεδομένα από την συσκευή σε 6 domains (api.acuweather.com, dbank.com, clients4.google.com, csi.gstatic.com, hicloud.com και ccpc-cn.consumer.huawei.com). Τα domain accuweather και hicloud καταχωρούνται ως διαφημιστικά ή κατασκοπευτικά. Για το κομμάτι των διαρροών το Lumen παρουσιάζει διαρροή του build Fingerprint στο domain dbankcdn.com.

Όπως θα παρουσιαστεί και πιο κάτω παρά την μεγάλη σε έκταση περίοδο που έγινε το M.I.T.M. και τις δεκάδες χιλιάδες ροές που μελετήθηκαν, δεν βρέθηκε καμία για το domain dbankcdn.com αλλά και για το huawei.com. Επίσης σημαντικό είναι να τονιστεί ότι η

περίοδος που έγινε η αξιολόγηση (μέσω του M.I.T.M.) είναι μετά την περιβόητη απαγόρευση συνεργασίας όλων των αμερικάνικων εταιριών με την Huawei. [24]



Εικόνα 30. OWASP ZAP – όπως και σε όλες τις προηγούμενες εφαρμογές που εξετάστηκαν η Google για ακόμα μια φορά μέσω της πλατφόρμας της καταχωρεί και επεξεργάζεται κρυπτογραφημένα δεδομένα από την εφαρμογή Health (Huawei).

Εικόνα 31. OWASP ZAP – εδώ παρουσιάζεται μια ροή προς το domain hicloud.com που πραγματοποιείται από τα Mobile Services της Huawei που εγκαταστάθηκαν παράλληλα με την εφαρμογή Health.

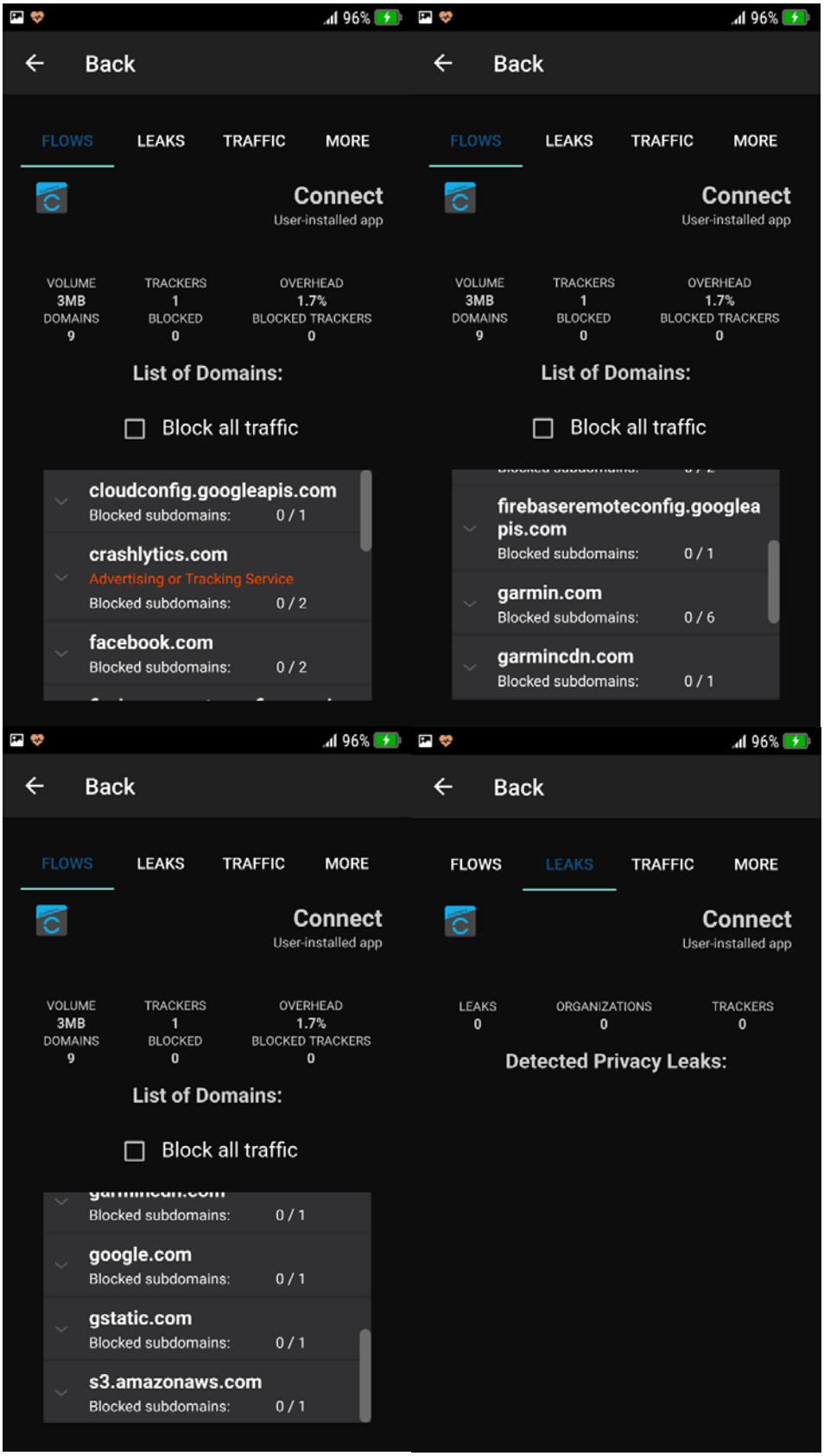
[24] https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

Το domain hicloud.com ανήκει στην Huawei και όπως φαίνεται στην Εικόνα 31 δεν φαίνεται να αποστέλλονται δεδομένα προσωπικού χαρακτήρα του χρήστη σε αυτή την βάση δεδομένων.

	api.acuweather.com	dbank.com	clients4.google.com	csi.gstatic.com	hicloud.com	ccpc-cn.consumer.huawei.com
Build Fingerprint			✓		✓	
Όνομα Συσκευής			✓		✓	
GAID						
Χώρα						
email						
Κρυπτογραφημένα			✓			

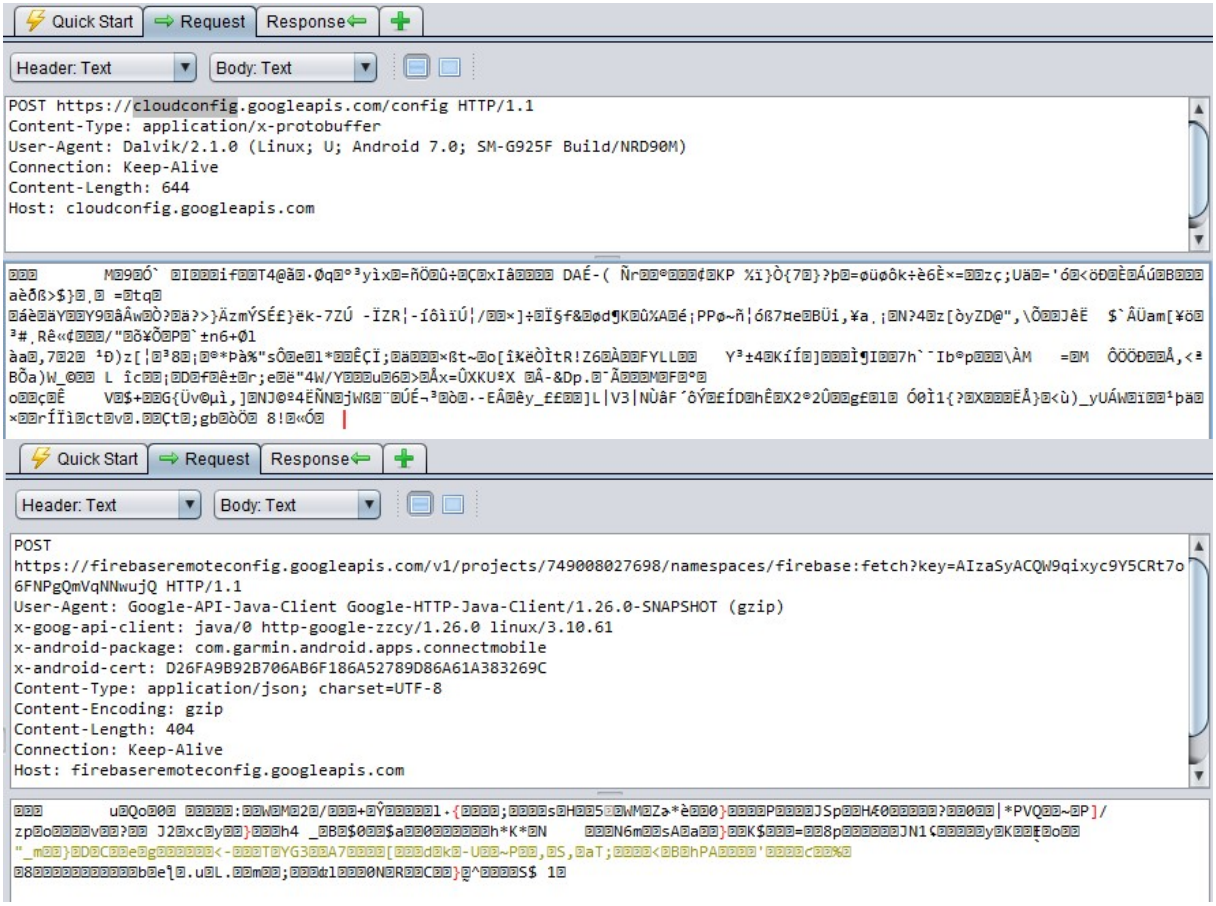
Πίνακας 6. Παρουσίαση δεδομένων προσωπικού χαρακτήρα που βρέθηκαν να συλλέγονται ανά domain στην εφαρμογή Huawei Health.

5.3.6 Garmin Connect

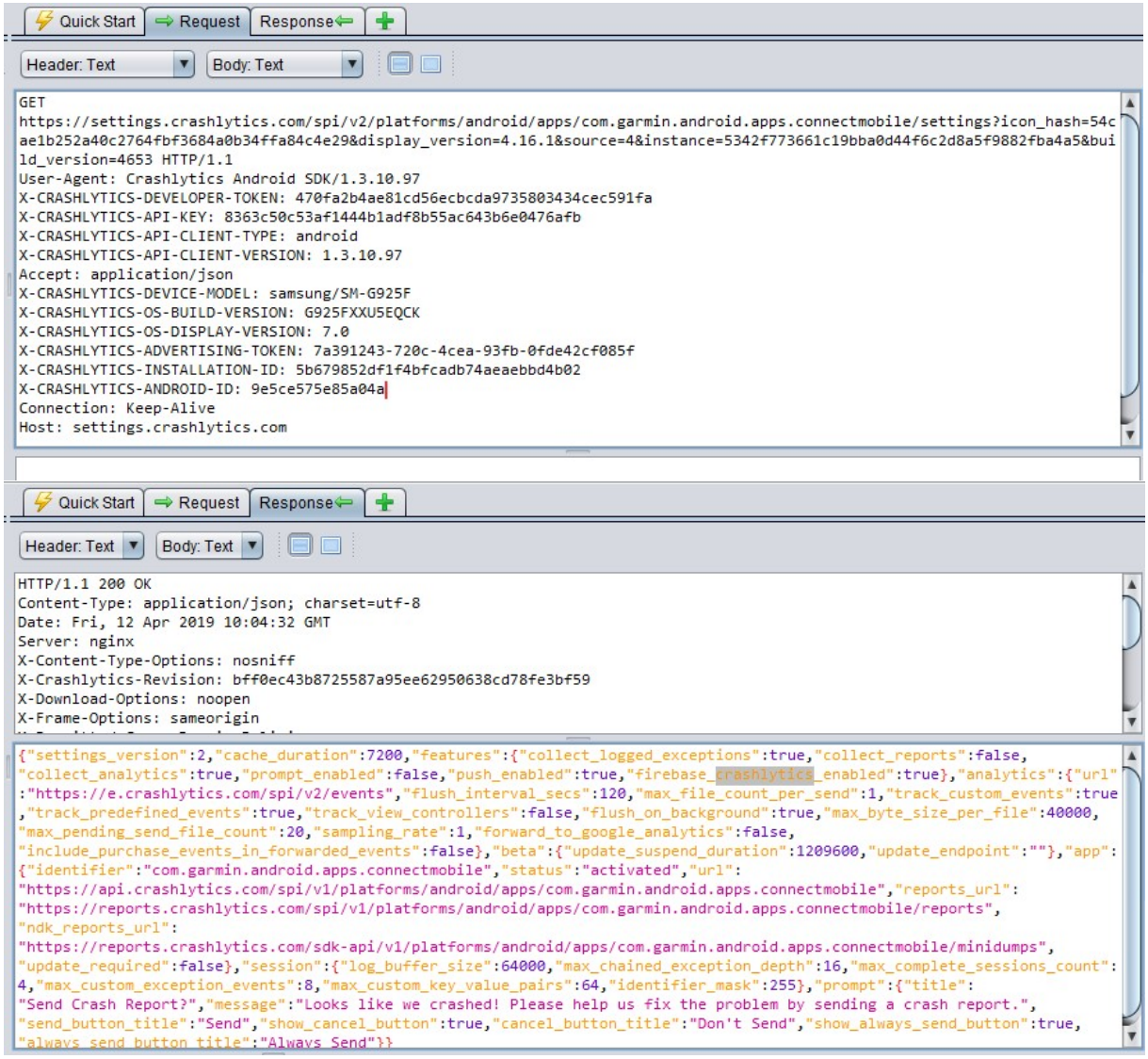


Εικόνα 32. Lumen - Παρουσιάζονται όλες οι ροές της εφαρμογής Health (Huawei) προς όλους τους servers όπως επίσης και μη διαρροή προσωπικών δεδομένων.

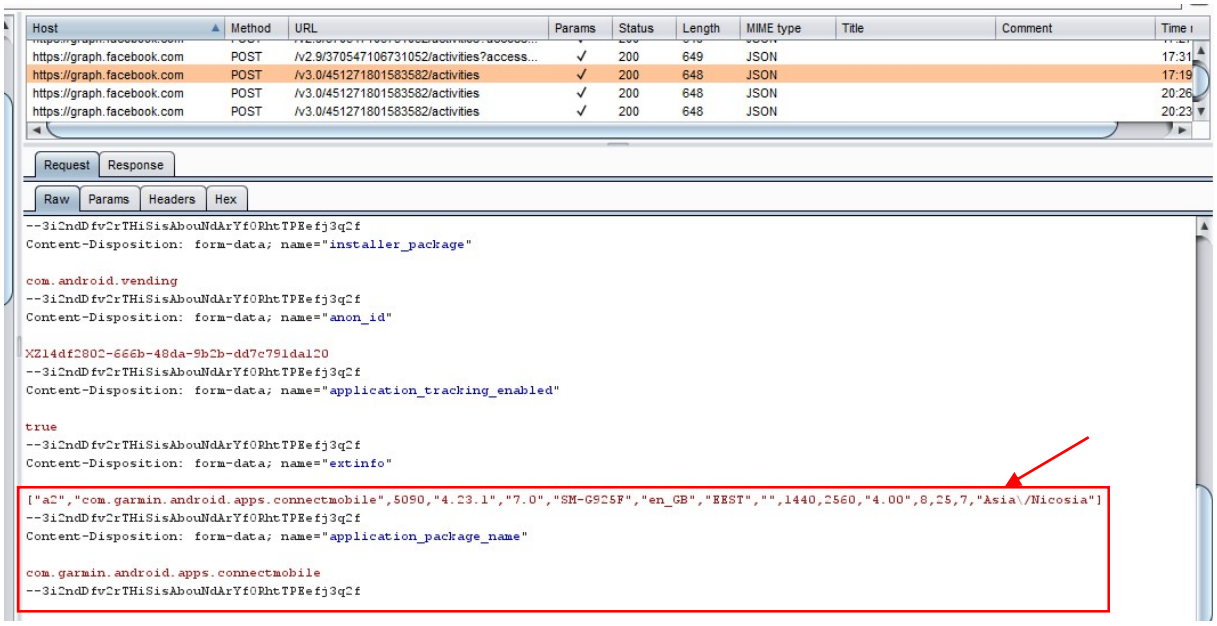
Η ανάλυση του Lumen, για την εφαρμογή Garmin Connect δείχνει ότι αποστέλλονται δεδομένα από την συσκευή σε 9 domains (googleapis.com, crashlytics.com, facebook.com, firebaseremoteconfig.googleapis.com, garmin.com, garmincdn.com, clients4google.com, cgi.gstatic.com, s3.amazonaws.com). Από όλα αυτά τα domains το Lumen χαρακτηρίζει το crashlytics ως διαφημιστικό ή κατασκοπευτικό. Στο κομμάτι των διαρροών δεδομένων προσωπικού χαρακτήρα δεν παρουσιάζει κάποιο αποτέλεσμα.



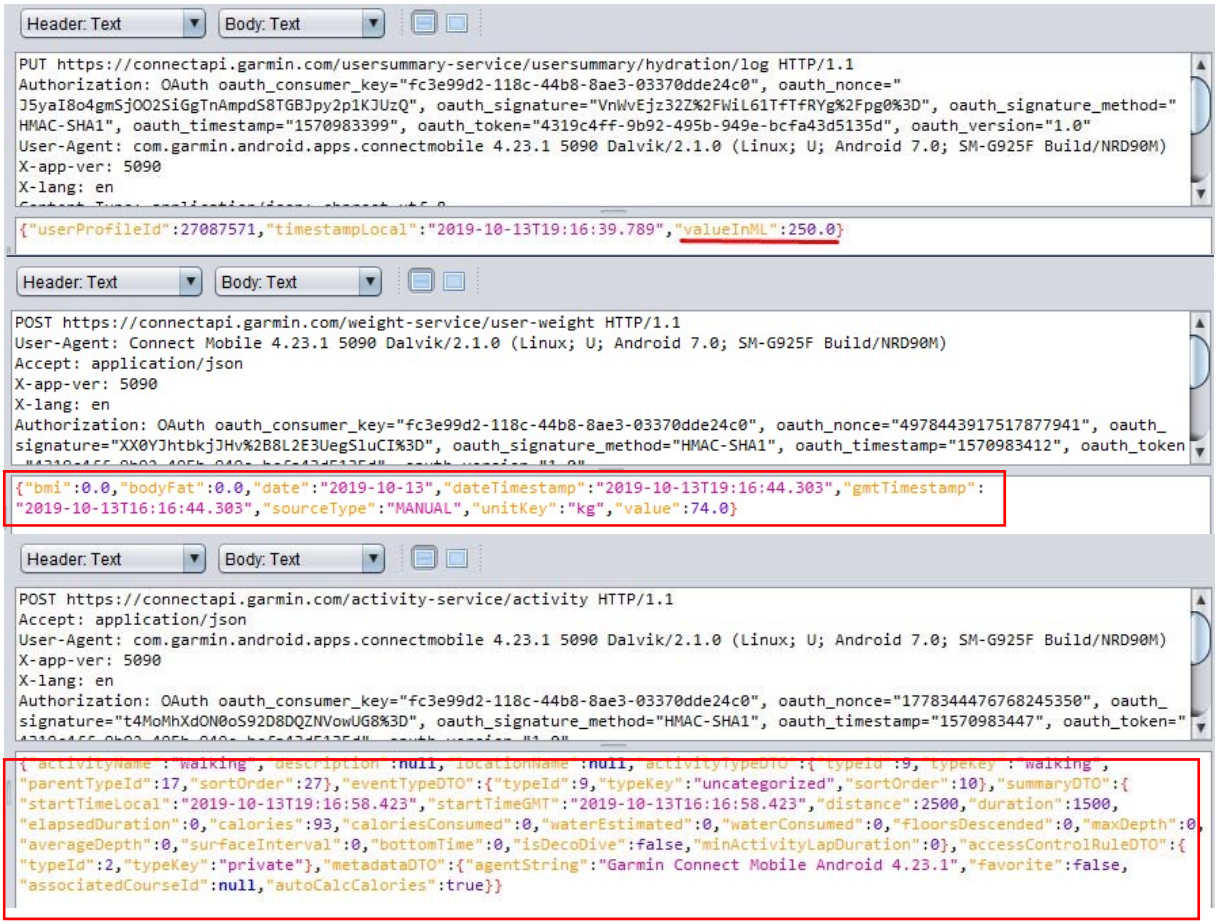
Εικόνα 33. OWASP ZAP – η Google όπως και σε όλα τα άλλα domain της, χρησιμοποιεί κρυπτογράφηση.



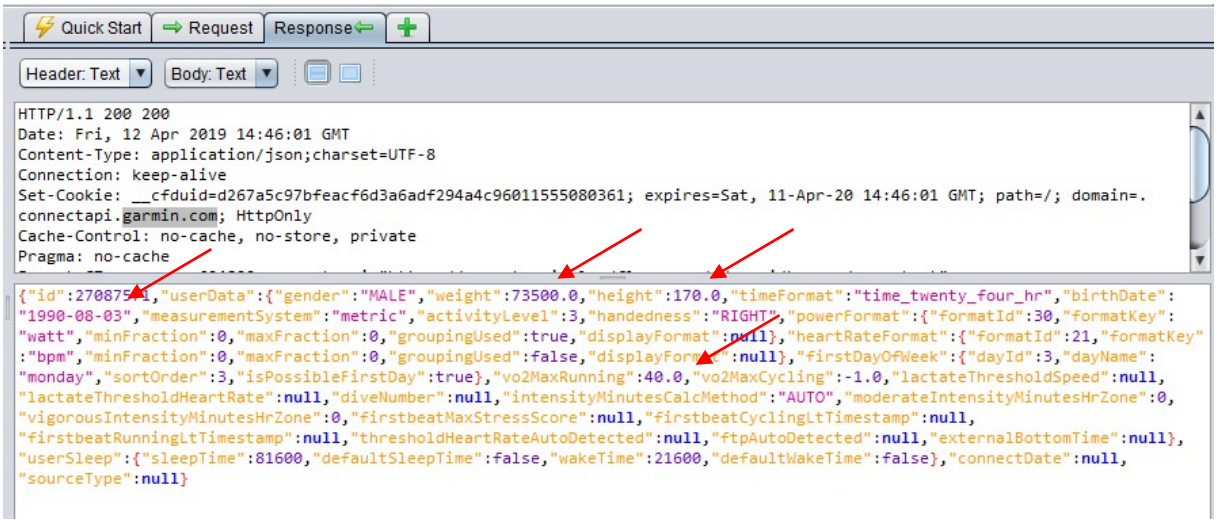
Εικόνα 34. OWASP ZAP – παρουσιάζεται ένα crash report το οποίο αποστέλλεται στο domain crashlytics που ανήκει στην Google.



Εικόνα 35. Burp Suite – Αποστέλλονται στο facebook στοιχεία της συσκευής, όπως και το GAID



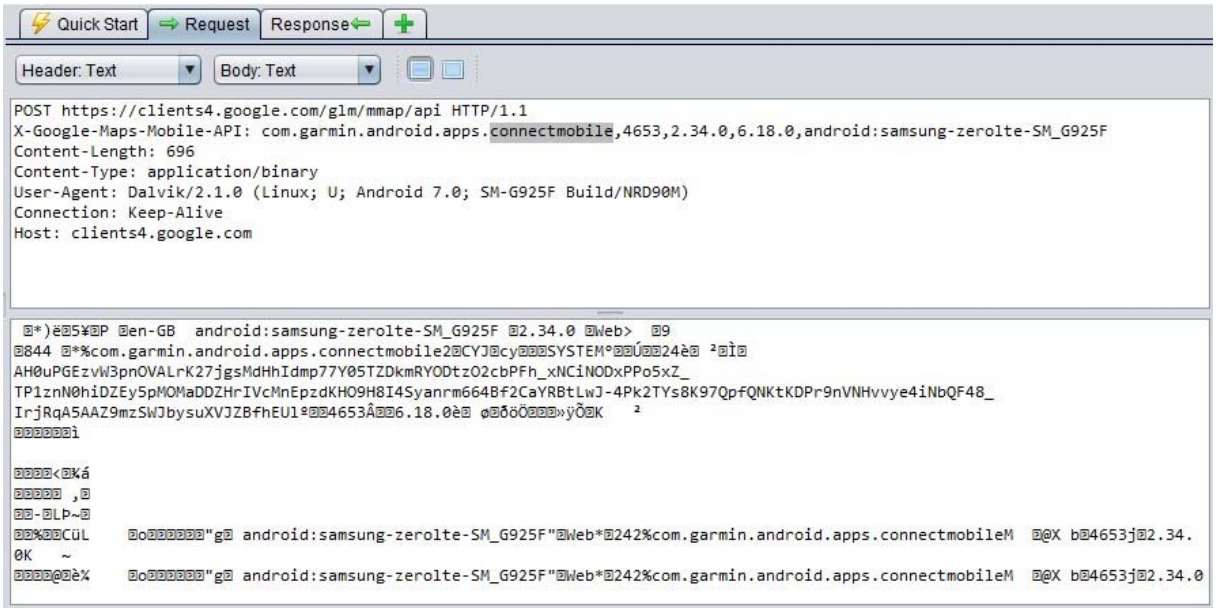
Εικόνα 36. Burp Suite – Δεδομένα που εισάγονται στην βάση δεδομένων της Garmin.



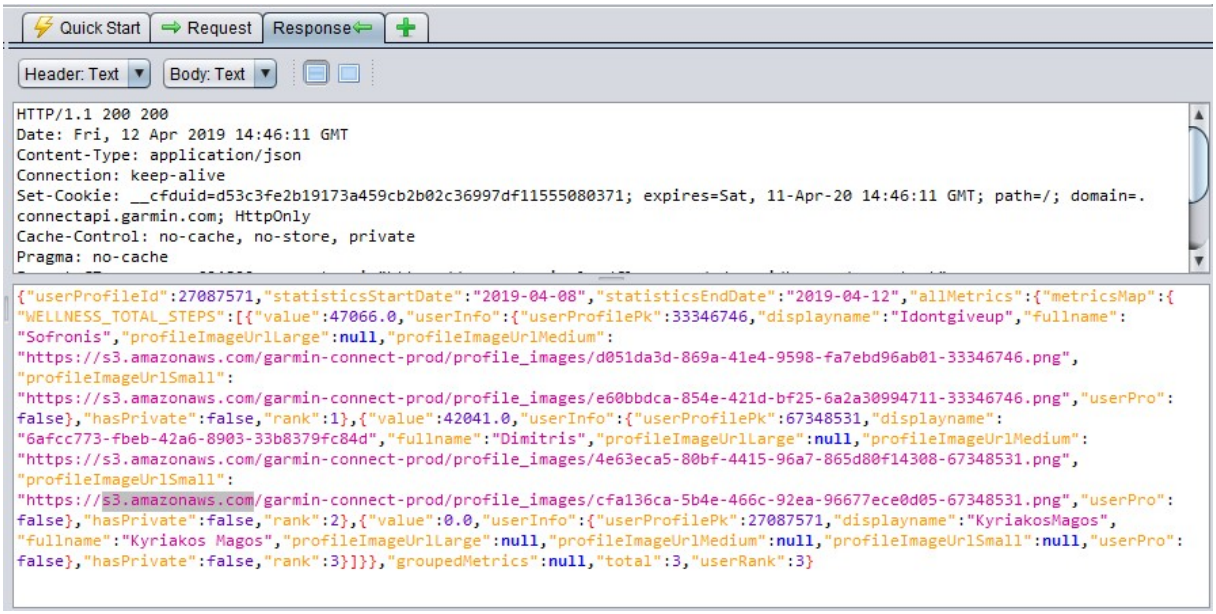
Εικόνα 37. Burp Suite – Δεδομένα που αποθηκεύονται στο cloud.

Εικόνα 38. Burp Suite – Δεδομένα που εισάγονται στην βάση δεδομένων της Garmin από την συσκευή Fenix 2.

Στις εικόνες πιο πάνω παρουσιάζονται αρκετά δεδομένα προσωπικού χαρακτήρα που εισάγονται στην βάση δεδομένων της Garmin. Στις εικόνες 36 και 37 παρουσιάζονται δεδομένα που εισήχθησαν μέσω της εφαρμογής Garmin connect. Όπως παρουσιάζουν οι ροές προς την βάση δεδομένων μεταξύ άλλων υπάρχουν πόσο νερό κατανάλωσε ο χρήστης, το βάρος του χρήστη αλλά και όλες οι πληροφορίες για μια δραστηριότητα του όπως το είδος της δραστηριότητας, ο χρόνος έναρξης, πόσο χρόνο διάρκεσε η δραστηριότητα, τι απόσταση διένυσε και πόσες θερμίδες κατανάλωσε. Στην εικόνα 38 όμως παρουσιάζεται μια δραστηριότητα όπως εισάγεται από την συσκευή Fenix 2. Αυτή περιλαμβάνει όλες τις προηγούμενες πληροφορίες συμπεριλαμβανομένου όμως της γεωγραφικής θέσης έναρξης και τερματισμού της δραστηριότητας, μέση ταχύτητα, μέγιστη ταχύτητα, υψόμετρο της δραστηριότητας, μέσους και μέγιστους καρδιακούς παλμούς κ.α.



Εικόνα 39. OWASP ZAP – όπως και σε όλες τις προηγούμενες εφαρμογές που εξετάστηκαν η Google για ακόμα μια φορά μέσω της πλατφόρμας της καταχωρεί και επεξεργάζεται κρυπτογραφημένα δεδομένα από την εφαρμογή Garmin Connect.



Εικόνα 40. OWASP ZAP – όπως φαίνεται η Garmin χρησιμοποιεί το domain amazonaws.com για να αποθηκεύει τις φωτογραφίες των χρηστών της. Το domain ανήκει στην Amazon.

	google apis.com	crashlytics.com	facebook.com	firebaseremoteconfig.googleapis.com	garmin.com	garmincdn.com	clients4google.com	cgi.gstatic.com	s3.amazonaws.com
Build Fingerprint	✓	✓	✓	✓	✓		✓	✓	
Όνομα Συσκευής	✓	✓	✓	✓	✓		✓	✓	
GAID			✓						
Τοποθεσία					✓				
Δεδομένα Υγείας και φυσικής κατάστασης					✓				
Δεδομένα Δραστηριότητας					✓				
Δεδομένα διατροφής					✓				
Φωτογραφία Χρήστη									✓
Κρυπτογραφημένα	✓			✓			✓		

Πίνακας 7. Παρουσίαση δεδομένων προσωπικού χαρακτήρα που βρέθηκαν να συλλέγονται ανά domain στην εφαρμογή Garmin Connect.

	googleapis.com	clients4google.com	gstatic.com	graph.facebook.com
Google Fit	✓	✓	✓	
Samsung Health		✓		
LG Health		✓		
Mi Fit		✓	✓	✓
Huawei Health		✓	✓	
Garmin Connect	✓	✓	✓	✓

Πίνακας 8. Παρουσίαση domain που βρέθηκαν σε περισσότερες από μια εφαρμογές .

Κεφάλαιο 6

Συμπεράσματα

6.1 Δεδομένα που συλλέγονται

Για την απάντηση στο πρώτο ερευνητικό ερώτημα (αν δεδομένα που συλλέγονται είναι αυτά που αναφέρει η αναφορά ιδιωτικότητας της εφαρμογής), σε συνάρτηση με όλη την ανάλυση των πιο πάνω, υπάρχει μια ξεκάθαρη εικόνα για το τι συλλέγεται και αποστέλλεται από κάθε εφαρμογή.

Αρχικά για την εφαρμογή Google Fit όπως παρουσιάστηκε στον έλεγχο της πολιτικής απορρήτου δεν εξακριβώνει τι δεδομένα συλλέγονται και επεξεργάζονται συγκεκριμένα για την εφαρμογή αυτή, αλλά έχει γενικά για όλες τις εφαρμογές και υπηρεσίες της Google, πράγμα που δεν βοηθά καθόλου για τον σκοπό της μεταπτυχιακής διατριβής. Ωστόσο κατά την φάση της αξιολόγησης της εφαρμογής βρέθηκε ότι όλο το traffic πήγαινε σε servers και libraries της Google. Στις πλείστες περιπτώσεις το traffic ήταν ήδη κρυπτογραφημένο πριν από το επίπεδο εφαρμογής (TCP/IP Application Layer, TLS) με αποτέλεσμα να αυξάνεται φυσικά η ασφάλεια των δεδομένων του χρήστη, αλλά να μην μπορούν να αξιολογηθούν τι είδους δεδομένα αποστέλλονται. Στο traffic που δεν ήταν κρυπτογραφημένο βρέθηκε να συλλέγονται στοιχεία όπως το GAID, η χώρα του χρήστη, το email του, όπως επίσης και το build fingerprint. Επίσης άξιο αναφοράς είναι ότι όλες οι εφαρμογές που αξιολογήθηκαν χρησιμοποιούσαν την βιβλιοθήκη clients4.google.com για επεξεργασία των δεδομένων τους, καταλήγοντας έτσι τα δεδομένα όλων των εφαρμογών στην Google. Τα δεδομένα αυτά σε όλες τις περιπτώσεις σε όλες τις εφαρμογές ήταν κρυπτογραφημένα.

Ακολούθως για την εφαρμογή της Samsung η ανάλυση του Lumen δείχνει να στέλνει δεδομένα μόνο σε domain της Samsung. Το ίδιο έγραφε και η πολιτική απορρήτου της Samsung, ωστόσο βρέθηκαν μέσω των άλλων 2 εφαρμογών της αξιολόγησης ότι υπήρχε επεξεργασία δεδομένων μέσα από την πλατφόρμα της Google. Επίσης όταν εισάγονταν οι τροφές που κατανάλωνε ο χρήστης, η εφαρμογή της Samsung έστελνε αυτά τα δεδομένα στην fatsecret από την οποία γινόταν η επεξεργασία δεδομένων. Ακολούθως η fatsecret ως βιβλιοθήκη τρίτου μέλους έστελνε πίσω στο Samsung Health πληροφορίες για την τροφή όπως θερμίδες και θρεπτικά συστατικά. Στο κομμάτι των δεδομένων προσωπικού χαρακτήρα, τα δεδομένα που βρέθηκαν να χρησιμοποιούνται και να επεξεργάζονται από την εφαρμογή της Samsung εντάσσονται σε αυτά που αναγράφονται στην πολιτική απορρήτου της εφαρμογής.

Στη συνέχεια η εφαρμογή LG Health όπως φαίνεται από τις αξιολογήσεις χρησιμοποιεί εξ ολοκλήρου την πλατφόρμα της Google για την επεξεργασία των δεδομένων. Όπως αναφέρθηκε προηγουμένως, σε όλες τις εφαρμογές παρατηρήθηκαν τα δεδομένα με τις δραστηριότητες του χρήστη να στέλνονται στην Google, κρυπτογραφημένα, για την επεξεργασία. Εδώ θα πρέπει να τονιστεί ότι η πολιτική απορρήτου της LG αναφέρει ότι περιορίζει τις λειτουργίες της εφαρμογής αναλόγως της χώρας του χρήστη και της εκάστοτε νομοθεσίας χωρίς να αναφέρει κάτι περισσότερο για την Κύπρο ή Ελλάδα συγκεκριμένα, αλλά και για τα δεδομένα που συλλέγει, τον σκοπό τους και τι επεξεργασίας τυγχάνουν. Επίσης άξιο αναφοράς είναι ότι η τελευταία ανανέωση της πολιτικής απορρήτου της εφαρμογής έγινε στις 31 Μαρ 2016 πολύ πριν της εφαρμογή του Γενικού Κανονισμού.

Η επόμενη εφαρμογή που εξετάστηκε είναι το Mi Health. Η εφαρμογή στο κομμάτι της συλλογής δεδομένων προσωπικού χαρακτήρα δεν παρεκκλίνει από την πολιτική απορρήτου της. Σε όλα τα δεδομένα που μελετήθηκαν δεν βρέθηκε πουθενά κάποιο από τα δεδομένα προσωπικού χαρακτήρα που να χρησιμοποίησε η εφαρμογή και να μην αναφέρεται στην πολιτική απορρήτου της. Ωστόσο δεν θα πρέπει να παραληφθεί ότι σε μερικές περιπτώσεις βρέθηκαν δεδομένα να εξέρχονται κρυπτογραφημένα χωρίς να μπορεί να προσδιοριστεί τι δεδομένα είναι αυτά.

Στην εφαρμογή της Huawei πάλι στο κομμάτι της συλλογής δεδομένων προσωπικού χαρακτήρα δεν παρατηρήθηκε οποιαδήποτε συλλογή δεδομένων εκτός από τις

κρυπτογραφημένες ροές δεδομένων προς το domain clients4.google.com. Εδώ θα πρέπει να τονιστεί ότι στις ρυθμίσεις της εφαρμογής δεν έχω αποδεχθεί τα δεδομένα να αποθηκεύονται στο cloud της Huawei Health (για σκοπούς πλήρης προστασίας της ιδιωτικότητας, αλλά και εξέτασης κατά πόσο η εφαρμογή θα τηρήσει αυτά που αναγράφει στην πολιτική απορρήτου), όπως αναφέρει και η πολιτική απορρήτου της εφαρμογής και όντως δεν παρατηρήθηκε οποιαδήποτε ροή προς οποιοδήποτε domain της Huawei.

Τέλος στην εφαρμογή Garmin Connect όπως και σε όλες τις υπόλοιπες δεν καταγράφηκαν δεδομένα προσωπικού χαρακτήρα που να συλλέχθηκαν ή να επεξεργάστηκαν και να μην αναφέρονται στην πολιτική απορρήτου.

Αφού έχουν αναλυθεί μια προς μια οι εφαρμογές αυτές μπορεί εύκολα να απαντηθεί το πρώτο ερευνητικό ερώτημα. Οι εταιρίες έχουν προσαρμόσει την πολιτική απορρήτου τους έτσι ώστε να αναφέρονται όλα τα δεδομένα που συλλέγουν χωρίς να αποκρύπτουν κανένα από αυτά. Μοναδική εξαίρεση αποτελεί η εφαρμογή της LG που η πολιτική απορρήτου έχει «ξεχαστεί» με αποτέλεσμα να μην καλύπτει την εφαρμογή σε καμία περίπτωση μετά την εφαρμογή του Γενικού Κανονισμού.

6.2 «Απαραίτητα» δεδομένα που συλλέγονται

Η απάντηση αυτής της ερώτησης δόθηκε εν μέρει στον προβληματισμό στο κεφάλαιο 3.2.4, αναλύοντας δηλαδή την συλλογή υπέρμετρων δεδομένων. Ωστόσο κάθε εφαρμογή στην πολιτική απορρήτου της, αναφέρει τον σκοπό για την επεξεργασία κάθε δεδομένου προσωπικού χαρακτήρα που συλλέγει (με εξαίρεση αυτή της LG). Προσδίδοντας στην πολιτική απορρήτου τον σκοπό της επεξεργασίας, παράλληλα με την ανάγκη συλλογής των δεδομένων αυτών από την κάθε εφαρμογή (για την ομαλή λειτουργία της εφαρμογής) καταστούν τα δεδομένα αυτά αναγκαία. Έτσι μελετώντας τα αποτελέσματα φαίνεται ότι οι εφαρμογές συλλέγουν αυτά που ορίζουν οι ίδιες ως απαραίτητα χωρίς όμως να σημαίνει ότι δεν θα μπορούσαν να λειτουργήσουν με λιγότερα δεδομένα από τον χρήστη.

6.3 Δεδομένα προς τρίτα μέλη

Για το κομμάτι αυτό θα γίνει ανάλυση για κάθε μια από τις εφαρμογές ξεχωριστά. Καταρχήν ο όρος τρίτο μέλος ή third party library ορίζει οποιοδήποτε domain ή βάση δεδομένων που

δεν ανήκει στην εταιρία ή όμιλο εταιριών αυτής που δημιούργησε την εφαρμογή ή/και συσκευή. Στις πολιτικές απορρήτου ωστόσο μόνο η Xiaomi και η Garmin αναφέρουν ξεκάθαρα ότι δεν θα παρέχονται δεδομένα σε τρίτους εκτός εάν υπάρχει ρητή συγκατάθεση του χρήστη για την ενέργεια αυτή. Οι Huawei και Samsung αν και αναγράφουν αρκετά περί ιδιωτικότητας και μέτρων ασφάλειας αυτής στο κομμάτι της παροχής προσωπικών δεδομένων σε τρίτους το προσπερνούν αθόρυβα.

Μια γενική παρατήρηση είναι ότι όλες οι εφαρμογές αποστέλλουν δεδομένα στην Google, κρυπτογραφημένα μεν, αλλά καμία δεν το αναφέρει στην πολιτική απορρήτου της. Είναι μια πολύ σοβαρή παράληψη διότι όχι μόνο αποθηκεύονται στης βάσεις δεδομένων της Google αλλά επίσης γίνεται επεξεργασία αυτών των δεδομένων από αυτή.

Οι εφαρμογές της Google και LG εκτός από την γενική παρατήρηση δεν παρατηρήθηκε με οποιαδήποτε εφαρμογή αποστολή δεδομένων σε τρίτους.

Η Samsung πέρα από την αποστολή δεδομένων στην Google, χρησιμοποιεί την πλατφόρμα της γνωστής fatsecret.com για να αντλήσει δεδομένα για την διατροφή του χρήστη. Σε καμία περίπτωση δεν ενημέρωνε τον χρήστη ότι τα δεδομένα διατροφής του θα επεξεργάζονταν από τρίτο ούτε υπήρχε η δυνατότητα για συγκατάθεση.

Η Xiaomi όπως ξαναειπώθηκε και πιο πάνω έστελνε δεδομένα στο κινέζικο amap.com (κρυπτογραφημένα) και facebook.com χωρίς την γνώση του χρήστη ενώ βρέθηκε και επικοινωνία με το κινέζικο qq.com και amazonaws.com χωρίς να παρατηρηθεί όμως αποστολή δεδομένων προσωπικού χαρακτήρα του χρήστη.

Αντίστοιχα στην εφαρμογή της Huawei δεν βρέθηκε οποιαδήποτε αποστολή δεδομένων σε τρίτους κατά την φάση της αξιολόγησης των δεδομένων από το M.I.T.M. ωστόσο το Lumen έδειξε αποστολή δεδομένων στο dbank.com που είναι μια κινέζικη βάση δεδομένων και στο hicloud.com που είναι εγγεγραμμένο στην Alibaba.

Τέλος στην Garmin βρέθηκε αποστολή δεδομένων στο facebook.com και στην amazonaws.com (όπου αποθηκεύει τις φωτογραφίες που εισάγουν οι χρήστες) χωρίς πάλι την γνώση και συγκατάθεση του χρήστη.

6.4 Εξαγωγή συμπερασμάτων για την υγεία του χρήστη

Για την απάντηση αυτής της ερώτησης θα πρέπει να ληφθούν υπόψη οι προβληματισμοί στα τμήματα 3.2.1, 3.2.4 και 3.2.5. Χρόνο με το χρόνο οι συσκευές ή/και εφαρμογές παρακολούθησης φυσικής κατάστασης προσφέρουν όλο και περισσότερες δυνατότητες είτε προσθέτοντας επιπρόσθετους αισθητήρες είτε αυξάνοντας την απόδοση τους είτε καταγράφοντας όλο και περισσότερα δεδομένα, προσπαθώντας να δώσουν το κάτι παραπάνω για τα αγοράσει ή/και αναβαθμίσει ένας χρήστης. Έτσι τα δεδομένα που δύναται να συλλέξουν αυτές οι συσκευές/εφαρμογές είναι αρκετά για την εξαγωγή συμπερασμάτων. Μερικά από τα δεδομένα υγείας που μπορεί να συλλέγουν είναι ηλικία, αριθμός βημάτων, καρδιακοί παλμοί, είδος άσκησης που κάνει ο χρήστης, ώρες που ασκείται χρόνος που ασκείται κ.α. Αφού επεξεργαστούν αυτά τα δεδομένα, λαμβάνοντας υπόψη ότι αυτά τα δεδομένα μπορούν να συνδυαστούν με δεδομένα από άλλους αισθητήρες όπως κάμερα, μικρόφωνο και GPS τότε είναι ασφαλές να υποθέσουμε ότι μπορούν να εξαχθούν συμπεράσματα όχι μόνο για την υγεία αλλά και για τις συνήθειες του κάθε ατόμου ξεχωριστά. Για παράδειγμα ο συνδυασμός των βημάτων με την ώρα και την τοποθεσία μπορούν να καταγράψουν συνήθειες των χρηστών ή ο συνδυασμός καρδιακών παλμών με τοποθεσίας και ώρας μπορεί να δώσει συμπεράσματα για την υγεία του χρήστη (εφόσον η τοποθεσία είναι σε κέντρο υγείας).

6.5 Δημιουργία προφίλ από τα δεδομένα που συλλέγονται

Στην ερώτηση αυτή ένας από τους στόχους ήταν να διαφανεί κατά πόσο συνδυάζοντας δυο ή περισσότερες βάσεις δεδομένων (third party libraries) θα αποτελούσε κίνδυνο για την ιδιωτικότητα του χρήστη και κατά πόσο αυτό θα ήταν ικανό να σκιαγραφήσει ένα προφίλ για αυτόν. Με γνώμονα ότι πλέον το πιο πολύτιμο πράγμα είναι η πληροφορία, και ότι αυτός που ελέγχει την πληροφορία μπορεί να ανεβάζει και να κατεβάζει κυβερνήσεις κυριολεκτικά (Cambridge Analytica), έτσι η υπέρμετρη συλλογή πληροφοριών καταστεί μια εταιρία κυρίαρχη. Όπως φαίνεται στον πίνακα 8 υπάρχουν βάσεις δεδομένων οι οποίες έχουν πρόσβαση σε περισσότερες από μια εφαρμογές συλλέγοντας έτσι πολλαπλάσια δεδομένα προσωπικού χαρακτήρα από τον χρήστη με πρώτη και καλύτερη την Google και το Facebook. Παρόλα αυτά λαμβάνοντας υπόψη τα ανωτέρω είναι φανερό ότι μια και μόνο βάση δεδομένων μπορεί να έχει αρκετά δεδομένα από τον χρήστη (αυτά που αναφέρει στην αναφορά ιδιωτικότητάς της) για να μπορέσει να εξάγει συμπεράσματα, να υπολογίσει

ιατρικές παθήσεις και να κατασκευάσει ένα προφίλ για κάθε χρήστη. Ο μόνος περιορισμός που έχει η κάθε βάση δεδομένων είναι το αντίστοιχο νομικό πλαίσιο της κάθε χώρας που υπονομεύει πως θα ασφαλίζονται τα δεδομένα και τι μπορεί να κάνει με αυτά. Όπου υπάρχουν αυστηρά νομοθετικά πλαίσια ο χρήστης προστατεύει την ιδιωτικότητά του, όμως όπου δεν υπάρχουν ο χρήστης θα αποτελεί προϊόν της κάθε εταιρίας που θα πωλείται και θα αγοράζεται και μάλιστα χωρίς την γνώση του.

Κεφάλαιο 7

Επίλογος

7.1 Γενικά

Η παρούσα διατριβή μελέτησε «έξυπνες» εφαρμογές φυσικής κατάστασης, ως προς τη σκοπιά των κινδύνων ιδιωτικότητας που ενδεχομένως προκύπτουν από τη χρήση τους. Όπως περιγράφηκε στο προηγούμενο κεφάλαιο, στο οποίο παρατίθενται τα συμπεράσματα της εν λόγω έρευνας, οι εφαρμογές αυτές πραγματοποιούν επεξεργασία προσωπικών δεδομένων η οποία είτε δεν είναι πλήρως διαφανής είτε θα μπορούσε να χαρακτηριστεί ως υπέρμετρη, σε σχέση με τις κυρίως υπηρεσίες που παρέχουν οι εν λόγω συσκευές.

7.2 Περιορισμοί της έρευνας

Παρόλο που μελετήθηκαν όσοι περισσότεροι τομείς των λειτουργιών των εφαρμογών γινόταν στο πλαίσιο που περιεγράφηκε ανωτέρω, είναι αδύνατον να μπορέσουν να εξεταστούν όλοι. Κάθε μια από τις εφαρμογές διαθέτει μια πλειάδα από δυνατότητες όπως καταγραφή διαφόρων αθλητικών δραστηριοτήτων (περπάτημα, τρέξιμο, κολύμβηση, σκι, ποδήλατο, κ.α.), καταγραφή διαφόρων τιμών όπως πίεσης αίματος, γλυκόζης αίματος, στρες, SpO_2 κ.α. (κάποιες τιμές προϋποθέτουν συσκευές από τρίτους για την καταγραφή). Παράλληλα σε καμία εφαρμογή δεν εξετάστηκε το «κοινωνικό» της κομμάτι (εφόσον η εφαρμογή προσφέρει τέτοια λειτουργία). Με βάση τα παραπάνω έγινε η πληρέστερη δυνατή αξιολόγηση των εφαρμογών ως προς το κομμάτι της ιδιωτικότητας και παρουσιάστηκαν τα αποτελέσματα.

Τα προγράμματα που χρησιμοποιήθηκαν για την αξιολόγηση είναι δωρεάν προγράμματα και δεν μπορεί να ισχυριστεί ο οποιοσδήποτε ότι σίγουρα έχουν καταγράψει όλες τις εξερχόμενες ροές (traffic) από το κινητό τηλέφωνο. Επίσης η εφαρμογή Lumen που ήταν εγκατεστημένη στο υπό εξέταση κινητό τηλέφωνο έχει από μόνη της τους δικούς της περιορισμούς, δεν προσφέρει αναλυτική αναφορά για τα δεδομένα που εξέρχονται παρά μόνο μια μικρή αναφορά για τον προορισμό τους και εάν έχει διαρροή προσωπικών δεδομένων. Πιθανώς εξάλλου η εν λόγω εφαρμογή να μην εντόπισε ή να μην αναγνώρισε κάποια εξερχόμενη κίνηση.

Στα αποτελέσματα βρέθηκαν εξερχόμενα traffic τα οποία ήταν ήδη κρυπτογραφημένα πριν από το Application Layer με αποτέλεσμα να μην μπορεί να καταγραφεί τι δεδομένα απέστελλαν στους servers που πήγαιναν.

7.3 Μελλοντική μελέτη

Η παρούσα μεταπτυχιακή διατριβή θα μπορούσε να εμπλουτιστεί εφαρμόζοντας την ίδια πειραματική διαδικασία με άλλη συσκευή που τρέχει νεότερη έκδοση του Android έτσι ώστε να διαφανεί κατά πόσο το Android σαν Λειτουργικό Σύστημα εφαρμόζει μέτρα για την προστασία της ιδιωτικότητας του κάθε χρήστη.

Επίσης θα μπορούσε η έρευνα να επεκταθεί χρησιμοποιώντας περισσότερες εφαρμογές και συσκευές όπως τις δημοφιλής Apple Heath/ iWatch, Fitbit κ.α. ξεφεύγοντας δηλαδή από το περιβάλλον Android και εξετάζοντας κατά πόσο στο iOS περιορίζονται τα δεδομένα που συλλέγονται από τις εφαρμογές και κατά πόσο οι υπόλοιπες εφαρμογές που θα εξεταστούν θα καταλήξουν στα ίδια συμπεράσματα με αυτά της παρούσας διατριβής.

Επιπρόσθετα αφού περάσει ένα εύλογο χρονικό πλαίσιο να ξαναγίνει η ίδια μελέτη, με την ίδια πειραματική διάταξη, για να διαφανεί κατά πόσο οι εταιρίες των εφαρμογών έχουν αναθεωρήσει τις πολιτικές απορρήτου έτσι ώστε να ανταποκρίνονται περισσότερο στην εκάστοτε νομοθεσία και να συγκριθεί τι δεδομένα συλλέγουν τότε με αυτά που παρουσιάστηκαν, τόσο στον όγκο όσο και στην ποικιλία. Παράλληλα να εξεταστεί εάν πάλι οι ίδιες εταιρίες (Google, Facebook) συλλέγουν δεδομένα προσωπικού χαρακτήρα από περισσότερες από μια εφαρμογές και να επανεξεταστεί κατά πόσο με τα δεδομένα που

συλλέγονται μπορούν να εξάγουν συμπεράσματα για την υγεία του χρήστη ή/και να μπορούν να καταρτίσουν ένα προφίλ για τον χρήστη.

Σε κάθε περίπτωση, τα αποτελέσματα της έρευνας κατατείνουν σε ένα γενικό συμπέρασμα ότι πολλά μένουν ακόμα να γίνουν για την προστασία των προσωπικών δεδομένων στο χώρο των «έξυπνων» εφαρμογών. Οι εμπλεκόμενοι είναι πολλοί και διαφορετικοί (πάροχοι λειτουργικών συστημάτων, προγραμματιστές εφαρμογών, προγραμματιστές βιβλιοθηκών που μπορούν να χρησιμοποιηθούν ως τρίτα μέλη (third parties)), και απαιτείται από τον καθένα ξεχωριστά να δίνει έμφαση σε θέματα προστασίας δεδομένων: προς τούτο, κατάλληλες τεχνολογίες πρέπει να αναπτυχθούν (για παράδειγμα, το γεγονός ότι οι βιβλιοθήκες τρίτων μελών αποκτούν τα δικαιώματα της εφαρμογής η οποία τις έχει ενσωματώσει, το οποίο αποτελεί την τρέχουσα κατάσταση σε Android εφαρμογές, γεννά ζητήματα ιδιωτικότητας).

Βιβλιογραφία

Achara, J. P., V. Roca, C. Castelluccia, and A. Francillon. 2016. *MobileAppScrutinator: A Simple yet Efficient Dynamic Analysis Approach for Detecting Privacy Leaks across Mobile OSs*.

Arp, D., E. Quiring, C. Wressnegger, and K. Rieck. 2017. "Privacy Threats through Ultrasonic Side Channels on Mobile Devices." *IEEE Security and Privacy*.

Bauman, Z., and D. Lyon. 2013. *Liquid Surveillance: A Conversation*.

Chakravorti, B. 2018. "Why the Rest of the World Can't Free Ride on Europe's GDPR Rules." *Harvard Business Review*, April 30, 2018. https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules.

European Commision, Commision. 2018. "Τι είναι τα δεδομένα προσωπικού χαρακτήρα;" Text. Ευρωπαϊκή Επιτροπή - European Commission. 2018. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el.

European Parliament, Council of the European Union. 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." *Official Journal* L 281 (November): 31–50.

———. 1998. "Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector" OJ L (January). http://data.europa.eu/eli/dir/1997/66/oj/eng.

———. 2002. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)." *Official Journal* L 201 (July): 37–47.

———. 2009. "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws (Text with EEA Relevance)." *Official Journal of the European Union* L 337/11 (November). https://eur-lex.europa.eu/eli/dir/2009/136/oj/eng.

———. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance)." *Official Journal of the European Union* L 119/1 (May): 1–88.

Gadaleta, M., and M. Rossi. 2018. "IDNet: Smartphone-Based Gait Recognition with Convolutional Neural Networks." *Pattern Recognition* 74 (February): 25–37. https://doi.org/10.1016/j.patcog.2017.09.005.

Garmin. 2019. "Connect | Privacy Policy | Garmin." 2019. https://www.garmin.com/en-US/privacy/connect/policy/.

Github. 2015. "Android : Add Cert to System Store." Gist. 2015. https://gist.github.com/pwlin/8a0d01e6428b7a96e2eb.

Google. 2019. “Πολιτική Απορρήτου – Απόρρητο Και Όροι – Google.” 2019. https://policies.google.com/privacy.
Huawei. 2019. “Δήλωση Προστασίας Προσωπικών Δεδομένων - Huawei.” 2019. https://consumer.huawei.com/minisite/cloudservice/privacy/index.htm.
LG. 2016. “LG Health Privacy Policy.” 2016. https://health-api.lgfim.com/lifetracker/privacy/.
Montjoye, Y. A. de, C. A. Hidalgo, M. Verleysen, and V. D. Blondel. 2013. “Unique in the Crowd: The Privacy Bounds of Human Mobility.” *Scientific Reports* 3 (March): 1376.
Samsung. 2018. “Samsung Health Privacy Policy.” 2018. http://health.apps.samsung.com/policy.
Warren, S. D., and L. D. Brandeis. 1890. “The Right to Privacy.” *Harvard Law Review* 4 (5): 193–220. https://doi.org/10.2307/1321160.
Xiaomi. n.d. “Mi Fit User Agreement and Privacy Policy.” Accessed September 7, 2019. http://cdn.awsbj0.fds.api.mi-img.com/mifit/1480831742.html.