

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



Τίτλος Εργασίας:

«Μελέτη και ανάλυση των αδειών πρόσβασης και των πολιτικών ιδιωτικότητας των πιο επιτυχημένων εφαρμογών Android στο Google Play»

Όνομα φοιτήτριας : Μαλακούδη Κατερίνα

ΑΜ Φοιτήτριας : Π2013028

Επιβλέπουσα Καθηγήτρια: Τσώχου Αγγελική

Τριμελής Επιτροπή: Κουρουθανάσης Παναγιώτης
Μάγκος Εμμανουήλ

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την καθηγήτρια μου, κ. Αγγελική Τσώχου για την καθοδήγηση της, καθ' όλη τη διάρκεια της συγγραφής της πτυχιακής μου, αλλά και την οικογένεια μου για την ηθική και υλική υποστήριξη που μου παρείχε.

Πίνακας Περιεχομένων

Εξώφυλλο	0
Ευχαριστίες.....	1
Περίληψη.....	2
Κατάλογος Εικόνων.....	2
Κατάλογος Πινάκων.....	3
Πίνακας Περιεχομένων	3
1.Εισαγωγή	7
1.1 Εισαγωγικά.....	7
1.2 Ιστορική Ανασκόπηση του Android.....	7
1.3 Σκοπός της Εργασίας	8
1.4 Ανασκόπηση υπάρχουσας βιβλιογραφίας.....	8
2.Προστασία Δεδομένων Προσωπικού Χαρακτήρα	9
2.1 Ιδιωτικότητα.....	9
2.2 Νομική Διάσταση	10
2.3 Διαφορά Προσωπικών Δεδομένων και Ιδιωτικότητας	15
2.4 Πολιτικές Ιδιωτικότητας στις Εφαρμογές.....	16
3. Μοντέλα Αδειών Πρόσβασης.....	18
3.1 Android και Άδειες Πρόσβασης	18
3.2 Επίπεδα Προστασίας των Αδειών Πρόσβασης	18
3.3 Οι Αλλαγές στο Marshmallow Android 6.0	22
3.4 Μειονεκτήματα των Αδειών Πρόσβασης στο Android	23
4. Μεθοδολογία Εργασίας.....	24
4.1 Υλοποίηση.....	24
4.2 Εργαλεία.....	25
4.3 Μελέτη των Πολιτικών Ιδιωτικότητας Δέκα Δημοφιλών Εφαρμογών Android ως προς τα Δεδομένα που Συλλέγουν.....	38
4.4 Αποτελέσματα και Συγκρίσεις από τη Μελέτη των Πολιτικών Ιδιωτικότητας των Δέκα πιο Επιτυχημένων Εφαρμογών	58
4.5 Αποτελέσματα από την Εκτέλεση των SQL Ερωτημάτων	71
5. Συμπεράσματα.....	85
6.Επίτευξη Στόχων Πτυχιακής και Μελλοντικές Προσθήκες.....	87
Βιβλιογραφία	88
Παράρτημα Α.....	91

Περίληψη

Κύριο αντικείμενο έρευνας της παρούσας εργασίας αποτελεί η ιδιωτικότητα των χρηστών των εφαρμογών Android. Ο λόγος που ώθησε τη συγγραφέα να ασχοληθεί με το συγκεκριμένο αντικείμενο είναι η επιτακτική ανάγκη ενίσχυσης της προστασίας των προσωπικών δεδομένων των χρηστών αλλά και η αφύπνιση τους όσον αφορά τα προσωπικά στοιχεία που κοινοποιούν, τις άδειες πρόσβασης που παραχωρούν και τις εφαρμογές που επιλέγουν να εγκαταστήσουν.

Η παρούσα πτυχιακή χωρίζεται σε δυο μέρη όπου το πρώτο ασχολείται με τη μελέτη και την ανάλυση των αδειών πρόσβασης που απαιτούν οι εφαρμογές Android από κάθε χρήστη. Για την άντληση των δεδομένων των εφαρμογών από το Google Play, υλοποιήθηκε μια προγραμματιστική εφαρμογή σε C#, με το οποίο και συλλέχθηκαν στοιχεία όπως το όνομα, το url και τις άδειες πρόσβασης που ζητά από τους χρήστες, κάθε εφαρμογή. Οι εφαρμογές επιλέχθηκαν από το επίσημο market της Google, το Google Play Store, από 32 διαφορετικές κατηγορίες και ο αριθμός αυτών αγγίζει τις 3026. Αφ' ότου έγινε η συλλογή των στοιχείων για κάθε εφαρμογή, αυτά καταχωρήθηκαν σε μια βάση δεδομένων sqlite. Στη συνέχεια, υλοποιήθηκαν SQL ερωτήματα ή αλλιώς Queries στη βάση δεδομένων έτσι ώστε να γίνει εξαγωγή αποτελεσμάτων και στη συνέχεια συμπερασμάτων αναφορικά με τις άδειες πρόσβασης αλλά και τις εφαρμογές.

Τα αποτελέσματα τα οποία σχηματίστηκαν μέσω των Queries, δημιουργούν ερωτήματα στους αναγνώστες και εν δυνάμει χρήστες, καθώς παρατηρούμε πως οι περισσότερες άδειες που ζητούνται από τις εφαρμογές ανήκουν στις επικίνδυνες άδειες, και οι εφαρμογές που τις ζητούν, πολλές φορές δεν χρειάζονται τον υπέρογκο αριθμό των αδειών αυτών.

Όσον αφορά το δεύτερο μέρος της πτυχιακής, το οποίο σχετίζεται με τις πολιτικές ιδιωτικότητας των δέκα πιο επιτυχημένων εφαρμογών του Google Play που μελετήσαμε, καταλήξαμε στο συμπέρασμα ότι οι περισσότερες εφαρμογές παρουσιάζουν κενά στις πολιτικές τους και ειδικότερα στην αναφορά των δεδομένων που συλλέγουν. Μετά τη μελέτη των πολιτικών, συμπεραίνουμε ότι, από τις δέκα αυτές επιτυχημένες εφαρμογές, η πολιτική της εφαρμογής η οποία παρουσιάζεται πιο ελλιπής είναι αυτή του Browser Mozilla Firefox. Από την άλλη πλευρά, οι πολιτικές των εφαρμογών Facebook, WhatsApp και Netflix, κρίθηκαν οι πιο επεξηγηματικές και σαφείς προς τους χρήστες.

Συνεπώς, τα συμπεράσματα που αντλούνται μέσα από τη συγκεκριμένη εργασία, αφυπνίζουν τους αναγνώστες όσον αφορά την ιδιωτικότητα τους και απαντούν στα ερωτήματα και τους προβληματισμούς των χρηστών αναφορικά με τις άδειες πρόσβασης και το σκοπό χρήσης αυτών από τις εφαρμογές. Παράλληλα, οι αναγνώστες και χρήστες βρίσκονται σε θέση να επιλέξουν με μεγαλύτερη σύνεση τις εφαρμογές που θα εγκαταστήσουν, βασιζόμενοι στις γνώσεις που αποκόμισαν από την παρούσα πτυχιακή εργασία.

Κατάλογος Εικόνων

Εικόνα 1. Οι πίνακες της βάσης δεδομένων.

Εικόνα 2. Ο πίνακας Apps της βάσης δεδομένων.

Εικόνα 3. Ο πίνακας AppsPermissions της βάσης δεδομένων.

Εικόνα 4. Οι επιμέρους άδειες πρόσβασης της κατηγορίας αδειών πρόσβασης Contacts στον πίνακα AppsPermissionsDetail.

Εικόνα 5. Ο πίνακας AppsPermissionsDetail .

Εικόνα 6. Ο πίνακας Categories της βάσης δεδομένων.

Εικόνα 7. Ο πίνακας OsPermissions της βάσης δεδομένων.

Λέξεις κλειδιά: Πολιτική Ιδιωτικότητας, Εφαρμογές Android, Προσωπικά Δεδομένα, Άδειες Πρόσβασης, Δικαιώματα Χρηστών, Ασφάλεια, Smartphones

Κατάλογος Πινάκων

- Πίνακας 1.** Χρονοδιάγραμμα του GDPR
- Πίνακας 2.** Οι καινοτομίες του Κανονισμού GDPR με λέξεις-κλειδιά
- Πίνακας 3.** Ποια δεδομένα ορίζονται ως προσωπικά σύμφωνα με την οδηγία 95/46/EK και το GDPR.
- Πίνακας 4.** Ενδεικτικά παραδείγματα παραβιάσεων ασφαλείας
- Πίνακας 5.** Κανονικές άδειες
- Πίνακας 6.** Επικίνδυνες άδειες και ομάδες αδειών
- Πίνακας 7.** Άδειες με υπογραφή
- Πίνακας 8.** Οι πίνακες της βάσης δεδομένων.
- Πίνακας 9.** Ο πίνακας Apps της βάσης δεδομένων.
- Πίνακας 10.** Δεδομένα που αντλεί η εφαρμογή Facebook .
- Πίνακας 11.** Δεδομένα που αντλεί η εφαρμογή Twitter.
- Πίνακας 12.** Δεδομένα που αντλεί η εφαρμογή Viber.
- Πίνακας 13.** Δεδομένα που αντλεί η εφαρμογή WhatsApp.
- Πίνακας 14.** Δεδομένα που αντλεί η εφαρμογή Netflix.
- Πίνακας 15.** Δεδομένα που αντλεί η εφαρμογή Stremio.
- Πίνακας 16.** Δεδομένα που αντλεί η εφαρμογή Google Chrome.
- Πίνακας 17.** Δεδομένα που αντλεί η εφαρμογή Mozilla Firefox.
- Πίνακας 18.** Δεδομένα που αντλεί η εφαρμογή Skype.
- Πίνακας 19.** Δεδομένα που αντλεί η εφαρμογή Zoom.
- Πίνακας 20.** Αριθμός εφαρμογών που μελετήθηκαν ανά κατηγορία του Google Play.
- Πίνακας 21.** Πλήθος αδειών πρόσβασης ανά εφαρμογή.
- Πίνακας 22.** Πλήθος αδειών ανά κατηγορία.
- Πίνακας 23.** Οι 40 εφαρμογές που ζητούν τα περισσότερα δικαιώματα.
- Πίνακας 24.** Οι 30 εφαρμογές που ζητούν τα λιγότερα δικαιώματα.
- Πίνακας 25.** Οι 30 εφαρμογές που ζητούν τις περισσότερες επικίνδυνες άδειες.
- Πίνακας 26.** Οι 30 άδειες που ζητούνται περισσότερο από τις εφαρμογές.
- Πίνακας 27.** Αντιστοίχιση των 30 αδειών με τις άδειες του λειτουργικού συστήματος Android.
- Πίνακας 28.** Οι 30 άδειες που ζητούνται λιγότερο από τις εφαρμογές.
- Πίνακας 29.** Οι 30 άδειες που ζητούνται περισσότερο και το ποσοστό των εφαρμογών που τις ζητούν
- Πίνακας 30.** Οι επικίνδυνες άδειες και το ποσοστό εφαρμογών που τις ζητούν.

1.Εισαγωγή

1.1 Εισαγωγικά

Η κυριαρχία των smartphones, γνωστών και ως έξυπνων τηλεφώνων είναι εμφανής αφού εξυπηρετούν και καλύπτουν κάθε ανάγκη του χρήστη, σε καθημερινή βάση. Τα κινητά τηλέφωνα ξεκίνησαν να παρέχουν απλές λειτουργίες όπως κλήση, μήνυμα και ραδιόφωνο, πλέον όμως, ο χρήστης μέσω αυτών, μπορεί να έχει πρόσβαση στο Internet, να συνδέεται στα κοινωνικά του δίκτυα επικοινωνώντας με ανθρώπους σε άλλη ήπειρο, να διαχειρίζεται τα email του, να φωτογραφίζει ή και να βιντεοσκοπεί. Αυτές είναι μόνο λίγες από την πληθώρα λειτουργιών που μπορεί ένα smartphone να προσφέρει στο χρήστη, οι οποίες όμως τις περισσότερες φορές είναι εφαρμογές από τρίτες οντότητες και πρέπει να εγκατασταθούν στο smartphone για να γίνει η χρήση τους. Για την εγκατάσταση των εφαρμογών αυτών πρέπει η συσκευή να διαθέτει ένα λειτουργικό σύστημα. Τα πιο γνωστά λειτουργικά συστήματα με σειρά επιτυχίας είναι το Android, iOS και Windows. Σύμφωνα με έρευνα που έγινε μεταξύ 2018-2019 οι χρήστες των συσκευών Android παγκοσμίως αγγίζουν το 74,45% ενώ οι χρήστες iOS το μόλις 22,85%. [\[1\]](#)

1.2 Ιστορική Ανασκόπηση του Android

Το καλοκαίρι του 2005 η Google εξαγόρασε την Android, μια μικρή εταιρεία η οποία τότε, είχε δημιουργήσει ένα λογισμικό για κινητά τηλέφωνα. Οι ιδρυτές του Android Inc. είχαν ξεκινήσει να αναπτύσσουν ένα εξελιγμένο λογισμικό για ψηφιακές φωτογραφικές μηχανές, όμως γρήγορα στράφηκαν στο λογισμικό κινητών τηλεφώνων, αφού η αγορά των φωτογραφικών μηχανών δεν ήταν τόσο μεγάλη.

Η δημιουργία του λογισμικού Android, βασίστηκε στο λειτουργικό σύστημα Linux και οι ανταγωνιστές του Android τότε, ήταν οι Symbian και Microsoft Windows Mobile.

Το Android κατάφερε να αποτελέσει το κύριο λειτουργικό σύστημα των τηλεφώνων της νέας γενιάς, αφού σε συνεργασία με πολλούς κατασκευαστές κινητής τηλεφωνίας δημιούργησε το πιο εξελιγμένο και ευέλικτο λειτουργικό σύστημα. Το πρώτο εμπορικά διαθέσιμο smartphone με λειτουργικό Android ήταν το HTC Dream, γνωστό και ως T-Mobile G1, το οποίο βγήκε σε κυκλοφορία στις 23 Σεπτεμβρίου 2008.

Οι εκδόσεις του λογισμικού παίρνουν ονόματα από γλυκά με την πρώτη έκδοση να ονομάζεται Donut και την τελευταία μέχρι στιγμής, Q(v.10). [\[2\]](#)

1.3 Σκοπός της Εργασίας

Όπως αναφέραμε, το Android αποτελεί το πιο επιτυχημένο λειτουργικό σύστημα με πάνω από 2,87 δισεκατομμύρια εφαρμογές προς εγκατάσταση. [3] Οι εφαρμογές αυτές όμως, απαιτούν ορισμένες άδειες πρόσβασης, οι οποίες παρέχονται από το χρήστη όπως για παράδειγμα πρόσβαση στην τοποθεσία, τις επαφές, τον αποθηκευτικό χώρο, την κάμερα του. Τα δεδομένα που συλλέγονται από την εκάστοτε εφαρμογή, χρησιμοποιούνται είτε για την πραγματοποίηση κάποιας λειτουργίας της εφαρμογής, δηλαδή για παροχή υπηρεσιών, είτε για τη δημιουργία προφίλ του χρήστη, ακόμα και για το διαμοιρασμό των δεδομένων αυτών σε τρίτες συνεργαζόμενες οντότητες όπως διαφημιστές. Τεράστιος όγκος πληροφοριών αποθηκεύεται στα smartphones και ακόμα σε περίπτωση που αυτά δεν είναι ενεργοποιημένα παράγουν προσωπικές πληροφορίες, σημαντικές για την ιδιωτικότητα του χρήστη. Ο χρήστης δίνει τη συγκατάθεση του για την παροχή των προσωπικών του δεδομένων κατά τη λήψη και χρήση μιας εφαρμογής, όμως δεν υπάρχει πάντα πλήρης ενημέρωση από αυτήν, για τον σκοπό χρήσης των δεδομένων αυτών.

Σκοπός της παρούσας εργασίας είναι η μελέτη και η ανάλυση των αδειών πρόσβασης και των πολιτικών ιδιωτικότητας των εφαρμογών Android από το Google Play Market. Στόχος της εργασίας είναι η κατάληξη σε αξιόπιστα συμπεράσματα σχετικά με τις άδειες πρόσβασης που απαιτούν οι εφαρμογές του Google Play Market αλλά και η διερεύνηση των πολιτικών ιδιωτικότητας ορισμένων εφαρμογών απ' αυτές, ελέγχοντας την πληρότητα τους ως προς τις άδειες και τον τρόπο χρήσης τους.

1.4 Ανασκόπηση υπάρχουσας βιβλιογραφίας

Ερευνώντας για παρόμοιες εργασίες που αφορούν το αντικείμενο της παρουσίας πτυχιακής, δηλαδή τις άδειες πρόσβασης στις Android εφαρμογές, εντοπίστηκαν ορισμένες εργασίες οι οποίες αντλούν και επεξεργάζονται με διαφορετικό τρόπο τα δεδομένα των εφαρμογών απ' ότι η παρούσα πτυχιακή. Μια τέτοια εργασία είναι αυτή της Ματίνας Τσαβλή (2016) η οποία πραγματεύεται επίσης τα μοντέλα αδειών πρόσβασης, και αντλεί δεδομένα εφαρμογών, διαθέσιμων σε ΗΠΑ και Ελλάδα, μέσω μιας προγραμματιστής εφαρμογής υλοποιημένη σε Java. Ωστόσο, η εργασία αυτή συγγράφηκε το 2016 όπου το GDPR δεν είχε θεσπιστεί ακόμα και το Android Marshmallow μόλις είχε μπει σε ισχύ.

Παράλληλα, μια αξιοσημείωτη προσπάθεια αποτελεί ένα άρθρο των Hamed, Ayed και Machfar (2017) όπου μελετώνται οι άδειες πρόσβασης των εφαρμογών Android από την σκοπιά των κινδύνων που αυτές επιφέρουν. Στην εργασία αυτή, γίνεται μια προσέγγιση των κινδύνων του απορρήτου, αξιολογώντας τα δικαιώματα των εφαρμογών Android αλλά και παρουσιάζεται ένα δυναμικό μοντέλο το οποίο «προβλέπει» τον

κίνδυνο που θα επιφέρουν στο χρήστη, τα δικαιώματα της εκάστοτε εφαρμογής.

Ακόμη μια ερευνητική εργασία η οποία αφορά τις άδειες πρόσβασης και προέρχεται από τη συγγραφέα Fauzia Idrees Abro (2018), συμβάλλει στη βιβλιογραφία, με αντικείμενο τη διερεύνηση των αδειών πρόσβασης του Android και την ανίχνευση κακόβουλου λογισμικού. Η συγκεκριμένη εργασία προσεγγίζει διαφορετικά το πρόβλημα των αδειών πρόσβασης, ερευνώντας τη σύνδεση μεταξύ αδειών πρόσβασης και προθέσεων*. Επίσης με τη χρήση machine learning (μηχανικής μάθησης) ταξινομεί τις εφαρμογές κακόβουλου λογισμικού.

Συμπληρωματικά, μια έρευνα από τους Calciati και Kuznetsov πραγματεύεται την αδυναμία του Android, η οποία θίγεται και στην παρούσα πτυχιακή και αφορά την κατηγοριοποίηση των αδειών σε ομάδες αδειών. Ο χρήστης παρέχοντας πρόσβαση σε μια άδεια παρέχει πρόσβαση σε όλη την ομάδα αδειών, και δεν ενημερώνεται καν από το Android για περαιτέρω προσθήκες αδειών. Στην έρευνα αυτή, παρουσιάζονται οι κίνδυνοι που ελλοχεύουν οι ομάδες αδειών και πραγματοποιείται μια εμπειρική μελέτη σε 2.865.553 εφαρμογές, η οποία καταλήγει στο συμπέρασμα ότι τουλάχιστον το 17% των εφαρμογών, ζητά πρόσβαση από το λειτουργικό σύστημα σε νέες επικίνδυνες άδειες εν αγνοία του χρήστη.

Οι πτυχιακές εργασίες που αναφέρθηκαν, συμβάλλουν κατά πολύ στην εξερεύνηση του πεδίου των αδειών πρόσβασης και των κινδύνων που αυτές κρύβουν, ωστόσο λόγω της διαφορετικής αντιμετώπισης και μελέτης του πεδίου, κρίθηκε απαραίτητη η συνεισφορά μας στην υπάρχουσα βιβλιογραφία, με την παρούσα εργασία, αντλώντας δεδομένα, αναλύοντας τα, μελετώντας τις πολιτικές ιδιωτικότητας και καταλήγοντας σε συμπεράσματα με εναλλακτικό τρόπο από τους ήδη υπάρχοντες. Η άντληση των δεδομένων των εφαρμογών γίνεται μέσω της υλοποίησης προγράμματος σε γλώσσα C#, που δημιουργήθηκε αποκλειστικά για την παρούσα έρευνα, και στη συνέχεια η καταχώρηση και επεξεργασία των δεδομένων πραγματοποιείται σε βάση δεδομένων sqlite.

****Πρόθεση/Intent:** Μια πρόθεση στο λειτουργικό σύστημα Android είναι ένας μηχανισμός λογισμικού που επιτρέπει στους χρήστες να συντονίζουν τις λειτουργίες διαφορετικών δραστηριοτήτων για να επιτύχουν μια εργασία.

2.Προστασία Δεδομένων Προσωπικού Χαρακτήρα

2.1 Ιδιωτικότητα

Διάφοροι ορισμοί έχουν δοθεί κατά καιρούς έτσι ώστε να αποδώσουν την έννοια της ιδιωτικότητας και ο κάθε ορισμός προσδίδει και μια άλλη οπτική γωνία και διάσταση.

- ❖ Η ιδιωτικότητα μπορεί να οριστεί ως “η απόφαση του ατόμου για το πότε, που και σε ποιο βαθμό θα μεταδώσει τις πληροφορίες του σε άλλους”. [\[4\]](#)

- ❖ Η Οικουμενική Διακήρυξη για τα Ανθρώπινα δικαιώματα (1948) υποστηρίζει πως “κανείς δεν πρέπει να υποβάλλεται σε περιορισμό ή παράνομη επέμβαση στην ιδιωτική του ζωή, την οικογένεια, το σπίτι ή την αλληλογραφία του, ούτε να υπόκειται σε παράνομες προσβολές της τιμής και υπόληψης του. Επίσης, καθένας έχει δικαίωμα της έννομης προστασίας από κάθε είδους παρεμβάσεις και επιθέσεις” [\[5\]](#) (Άρθρο 12.1).
- ❖ Σύμφωνα με τους Warren and Brandeis (1890) σε ένα νομικό δοκίμιο που συνέγραψαν, ορίζουν την ιδιωτικότητα ως το “δικαίωμα του να είσαι μόνος” (the right to be let alone). [\[6\]](#)
- ❖ Ο Westin (1968) γράφει πως η ιδιωτικότητα “είναι το δικαίωμα του ατόμου να επιλέγει ελεύθερα χωρίς περιορισμούς το βαθμό προβολής των προσωπικών τους στοιχείων, τη στάση και τη συμπεριφορά τους απέναντι σε τρίτους” [\[7\]](#)
Κρίνοντας από τους προαναφερθείς ορισμούς των ειδικών, παρατηρούμε πως η έννοια της ιδιωτικότητας του ατόμου είναι υψίστης σημασίας και τα όρια της πρέπει να θέτονται σε κάθε περίπτωση από το άτομο το ίδιο.

2.2 Νομική Διάσταση

Ευρωπαϊκή Προσέγγιση

Υπάρχουν πολυπληθείς νόμοι, οι οποίοι ορίζουν την ιδιωτικότητα ως ύψιστο ανθρώπινο δικαίωμα της κάθε οντότητας.

- ❖ Το 1995, το Ευρωπαϊκό Κοινοβούλιο εξέδωσε την Οδηγία 95/46/ΕΚ για την προστασία των δικαιωμάτων βάσει της Ευρωπαϊκής Σύμβασης των Ανθρώπινων Δικαιωμάτων (Άρθρο 8) [\[8\]](#) και κάθε Ευρωπαϊκό κράτος έπρεπε να μεταφράσει την οδηγία σε εθνική νομοθεσία για την προστασία της ιδιωτικότητας. Στην προσπάθεια αυτή όμως, υπήρξαν κάποιες μικρές διαφορές στους νόμους κάθε χώρας, με αποτέλεσμα για παράδειγμα μια πολυεθνική εταιρεία να πρέπει να συμμορφωθεί διαφορετικά σε κανονισμούς ανάλογα με τη χώρα.

Άρθρο 8:

1. Παν προσώπου δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.

2. Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αυτή προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών

παραβάσεων, την προστασία της υγείας ή της ηθικής, ή την προστασία των δικαιωμάτων και ελευθεριών άλλων.



Πίνακας 1. Χρονοδιάγραμμα GDPR

πηγή: Βιβλίο Ειρηνικός Πλατής «Προσωπικά Δεδομένα-Προστασία GDPR.

Το πρόβλημα αυτό αποτέλεσε έναν από τους λόγους για τους οποίους, στις 25 Μαΐου του 2018 θεσπίστηκε από το Ευρωπαϊκό Κοινοβούλιο ο Γενικός Κανονισμός για την Προστασία Δεδομένων, γνωστός σε όλους ως GDPR. Ο κανονισμός αυτός, πήρε τη θέση της Οδηγίας 95/46/ΕΚ και αφορά όλες τις εταιρείες, οργανισμούς αλλά και τους δημόσιους κυβερνητικούς φορείς που επεξεργάζονται προσωπικά δεδομένα των πολιτών της Ευρωπαϊκής Ένωσης. Όλοι αυτοί οι οργανισμοί είχαν προθεσμία δυο χρόνων, από το 2016 μέχρι το 2018 έτσι ώστε να αλλάξουν τις πολιτικές τους σύμφωνα με το GDPR.

Παράλληλα, ένας από τους πιο σημαντικούς λόγους, ο οποίος συνετέλεσε στη θέσπιση του GDPR, αποτελεί η εξέλιξη της τεχνολογίας. Αν και από τα προηγούμενα χρόνια υπήρχε ανάγκη για την προστασία των προσωπικών δεδομένων, με την τεχνολογική εξέλιξη, η ανάγκη αυτή έγινε απαραίτητη, καθώς τα προσωπικά δεδομένα των χρηστών ξεκίνησαν να γίνονται προϊόν εκμετάλλευσης. Ένα απόσπασμα από το βιβλίο «EU General Data Protection Regulation (GDPR) : An Implementation and Compliance Guide», 2017, εξηγεί επακριβώς τους λόγους για τους οποίους η θέσπιση του GDPR, ήταν πλέον αναγκαία.

«Το GDPR είναι το τελευταίο βήμα της συνεχιζόμενης παγκόσμιας αναγνώρισης της αξίας και της σημασίας των προσωπικών πληροφοριών. Παρόλο που η αγορά των προσωπικών πληροφοριών υπήρχε ήδη για κάποιο χρονικό διάστημα, η πραγματική αξία των προσωπικών δεδομένων μόλις έγινε πιο προφανής. Η διαδικτυακή κλοπή δεδομένων προσωπικού χαρακτήρα εκθέτει τους πολίτες της Ε.Ε. σε σημαντικούς προσωπικούς κινδύνους. Μεγάλες τεχνικές

ανάλυσης δεδομένων επιτρέπουν στους οργανισμούς να ανιχνεύουν και να προβλέπουν την ατομική συμπεριφορά, η οποία μετέπειτα δύναται να αναπτυχθεί σε αυτοματοποιημένη λήψη αποφάσεων. Ο συνδυασμός όλων αυτών των ζητημάτων, σε συνδυασμό με τη συνεχή εξέλιξη της τεχνολογίας και τις ανησυχίες σχετικά με την κατάχρηση των προσωπικών δεδομένων από τις κυβερνήσεις και τις επιχειρήσεις, οδήγησε σε νέο νόμο της Ε.Ε. για τη διευκρίνιση των δικαιωμάτων των πολιτών της Ε.Ε. και για την εξασφάλιση κατάλληλου επιπέδου προστασίας των προσωπικών δεδομένων.»

✓ Ενίσχυση δικαιωμάτων υποκειμένων	✓ Αυστηριοποίηση κυρώσεων
✓ Ενίσχυση δικαιώματος στη λήθη	✓ Σύσταση Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων
✓ Θέσπιση δικαιώματος στη φορητότητα	✓ Θέσπιση μηχανισμού συνεκτικότητας
✓ Μεταφορά βάρους απόδειξης στους Υπευθύνους Επεξεργασίας (Λογοδοσία)	✓ Θεσμοθέτηση της Αρχής της Διαφάνειας

Πίνακας 2. Οι καινοτομίες του Κανονισμού GDPR με λέξεις-κλειδιά (Βαλαβάνης,2019)

Ελληνική Προσέγγιση

Στην Ελλάδα, η πρώτη προσπάθεια για την προστασία των προσωπικών δεδομένων υπήρξε με την επιτροπή Χαλαζωνίτη το 1985, στην οποία έγινε αναφορά στα υπερευαίσθητα δεδομένα. Σημαντικό γεγονός αποτέλεσε η επικύρωση της Σύμβασης 108 του Συμβουλίου της Ευρώπης με τη ψήφιση του νόμου 2068/1992. Το 1997, με τον νόμο 2472/1997 ξεκίνησε η διαδικασία προσαρμογής της Κοινοτικής Οδηγίας 95/46/ΕΚ της Ευρωπαϊκής Ένωσης στα Ελληνικά δεδομένα. Η Ελλάδα μάλιστα, προσπάθησε να υιοθετήσει τις αρχές και τις προβλέψεις της Οδηγίας με αυστηρό τρόπο, παρόλα αυτά οι αποκλίσεις του Νόμου από την αντίστοιχη Κοινοτική Οδηγία ήταν προφανείς και ουσιώδεις.

Το επόμενο βήμα πραγματοποιήθηκε το 2011, με τον Νόμο 3917/2011, στον οποίο αναφέρθηκε για πρώτη φορά η υποχρέωση των τηλεπικοινωνιακών παρόχων να προσφέρουν τις απαραίτητες πληροφορίες για την εξακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Επίσης, περιελάμβανε διατάξεις για την εδραίωση της προστασίας των ηλεκτρονικών επικοινωνιών του ελληνικού πληθυσμού, αλλά ακόμα και τρόπους με τους οποίους πρέπει να επεξεργάζονται τα δεδομένα οι πάροχοι, ορίζοντας τις υποχρεώσεις και τις ποινές τους σε περίπτωση μη συμμόρφωσης. Το 2013, νομιμοποιήθηκε η επεξεργασία των προσωπικών δεδομένων από τις δικαστικές αρχές και στη συνέχεια το 2016 η Ελλάδα όπως και όλα τα Ευρωπαϊκά κράτη μπήκαν στην τελική ευθεία για την καθολική εφαρμογή του Γενικού Κανονισμού Προσωπικών Δεδομένων.

Στην Ελλάδα του 2016, και όταν πλέον η ενίσχυση της προστασίας των προσωπικών δεδομένων είχε καταστεί αναγκαία, ψηφίστηκαν στις 27 Απριλίου δυο βασικά νομοθετήματα. Ο κανονισμός(ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα» ο οποίος τέθηκε σε εφαρμογή στις 25 Μαΐου του 2018 και η Οδηγία(ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου», για την ενσωμάτωση της οποίας στο εθνικό δίκαιο ορίστηκε προθεσμία έως τις 6 Μαΐου 2018. Στη συνέχεια, με κάποια σημαντική καθυστέρηση δημοσιεύεται ο νόμος 4624/2019, με τον οποίο και λαμβάνονται μέτρα εφαρμογής του Κανονισμού GDPR αλλά και ενσωματώνεται η Οδηγία. Έτσι, ο Γενικός Κανονισμός Προστασίας Δεδομένων τίθεται σε εφαρμογή στις 25 Μαΐου 2018 στην Ελλάδα, δημιουργώντας την αφετηρία ενός νέου “οδικού χάρτη” στη μακρά πορεία της προστασίας των προσωπικών δεδομένων, ο οποίος ισχύει και μέχρι σήμερα εν έτη 2020.

Διαφορές μεταξύ GDPR και Οδηγίας 95/46/ΕΚ :

- ❖ Ο κανονισμός GDPR είναι νόμος της ΕΕ με αποτέλεσμα όλα τα κράτη να έχουν την ίδια νομοθεσία και δεν χρειάστηκε μετάφραση σε εθνικές νομοθεσίες αφού δημιουργήθηκε με τρόπο τέτοιο έτσι ώστε να είναι εφαρμόσιμος σε όλες τις Ευρωπαϊκές χώρες.
- ❖ Οι οργανισμοί και εταιρείες με προσωπικό παραπάνω από 250 οφείλουν να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων(Data Protection Officer).
- ❖ Η οποιαδήποτε διαρροή δεδομένων πρέπει να δηλώνεται εντός 24 ωρών στην Εθνική Αρχή Προστασίας Δεδομένων.
- ❖ Τα ελλειπή μέτρα προστασίας των δεδομένων μπορούν να οδηγήσουν σε μεγάλα πρόστιμα που ανέρχονται στις δύο εκατοστιαίες μονάδες του παγκόσμιου κύκλου ή σε 10.000.000 ευρώ. Η Αρχή είναι ικανή επίσης, να αναστείλει τη λειτουργία ενός οργανισμού ή μιας εταιρείας αν κρίνει πως δεν συμμορφώνεται με τους κανονισμούς του GDPR.

Items That Constitute Personal Data	Data Protection Directive (1995)	General Data Protection Regulations (2018)
Name	✓	✓
Photo	✓	✓
E-mail Address	✓	✓
Phone Number	✓	✓
Address	✓	✓
Personal Identification Numbers	✓	✓
IP Addresses	✗	✓
Mobile Device Identifiers	✗	✓
Geo-Location	✗	✓
Biometric Data	✗	✓
Psychological Identity	✗	✓
Generic Identity	✗	✓
Economic Status	✗	✓
Cultural Identity	✗	✓
Social Identity	✗	✓

Πίνακας 3. Ποια δεδομένα ορίζονται ως προσωπικά σύμφωνα με την οδηγία 95/46/ΕΚ και το GDPR.

Πηγή: <https://coinaccord.io/blog/three-ways-data-protection-laws-will-affect-blockchain-organizations>

Αρχές Προστασίας Προσωπικών Δεδομένων

- ❖ *Αρχή του Προσδιορισμού του Σκοπού:* Είναι αναγκαίο να προσδιορίζεται, πριν τη συλλογή, ο σκοπός για τον οποίο γίνεται η συλλογή των δεδομένων. Ο σκοπός οφείλει να είναι νόμιμος και να προσδιορίζει τη συγκεκριμένη συλλογή και επεξεργασία χωρίς μεταβολές.
- ❖ *Αρχή του Περιορισμού της Συλλογής :* Είναι υποχρεωτικό να υπάρχουν όρια στη συλλογή των δεδομένων και η συλλογή να συμμορφώνεται με τη νομοθεσία ενημερώνοντας πάντα το χρήστη.
- ❖ *Αρχή της Ποιότητας των Δεδομένων:* Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν και να χαρακτηρίζονται από πληρότητα και ακρίβεια.
- ❖ *Αρχή του Περιορισμού της Χρήσης :* Τα δεδομένα δεν θα πρέπει να μοιράζονται σε τρίτες οντότητες ή σε συνεργαζόμενους οργανισμούς ή να χρησιμοποιούνται για άλλο σκοπό απ' αυτόν που έχει προσδιοριστεί, εκτός εάν υπάρχει συναίνεση του ατόμου είτε εξουσιοδότηση από το νόμο.
- ❖ *Αρχή της Προστασίας της Ασφάλειας :* Τα προσωπικά δεδομένα είναι αναγκαίο να προστατεύονται από κατάλληλους μηχανισμούς

ασφαλείας απέναντι σε κινδύνους όπως για παράδειγμα η μη εξουσιοδοτημένη χρήση, πρόσβαση, καταστροφή, τροποποίηση ή κοινοποίηση σε τρίτους.

- ❖ *Αρχή της Συμμετοχής του Ατόμου* : Το κάθε άτομο θα πρέπει να έχει το δικαίωμα :
 - i. Να ζητά από τον υπεύθυνο επεξεργασίας των δεδομένων, σε περίπτωση που διατίθενται, δεδομένα που σχετίζονται με το εν λόγω άτομο.
 - ii. Τα δεδομένα αυτά που ζητήθηκαν, να ανακοινώνονται σε σύντομο χρονικό διάστημα και με το λιγότερο κόστος.
 - iii. Σε περίπτωση που απορριφθούν οι αιτήσεις που αναφέρθηκαν πιο πάνω, να δίνεται στο άτομο η δυνατότητα αμφισβήτησης και διεκδίκησης των δεδομένων του.
 - iv. Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτόν.
- ❖ *Αρχή της Ευθύνης*: Ο υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα κάθε οργανισμού ή εταιρείας είναι υπόλογος όσον αφορά την εφαρμογή των μέτρων για να προαχθούν οι παραπάνω αρχές που διέπουν την προστασία των προσωπικών δεδομένων. [\[9\]](#)

2.3 Διαφορά Προσωπικών Δεδομένων και Ιδιωτικότητας

Πολλές φορές παρατηρείται η σύγχυση μεταξύ των εννοιών της ιδιωτικότητας και των προσωπικών δεδομένων και αυτό οφείλεται στην εξέλιξη του όρου της ιδιωτικότητας ως αξίας και σημασίας. Η σύγκληση αυτή είναι απόρροια των διαδικασιών που συνοδεύουν την παράλληλη εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών, την αποκέντρωση και διείσδυση της επεξεργασίας, και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας και όλων εκείνων των τεχνολογικών δραστηριοτήτων που συνεπάγονται σημαντικές αλλαγές στο περιβάλλον χρήσης της προσωπικής πληροφορίας. Συνεπώς, η σύγκλιση των δυο αυτών εννοιών συνδέεται με την τεχνολογική εξέλιξη και την επιτακτική ανάγκη προστασίας των ευαίσθητων δεδομένων μας, τα οποία ζητούνται καθημερινώς μέσα από τις ηλεκτρονικές συναλλαγές και τα κοινωνικά δίκτυα.

Παράλληλα, τα προσωπικά δεδομένα μπορούν να διαχωριστούν σε δυο είδη δεδομένων:

- ❖ Δεδομένα προσωπικού χαρακτήρα, αποτελεί κάθε πληροφορία και κάθε στοιχείο που αναφέρεται στο συγκεκριμένο άτομο.
- ❖ Ευαίσθητα δεδομένα, θεωρούνται τα δεδομένα που αφορούν φυλετική ή εθνική προέλευση, πολιτικά φρονήματα, θρησκευτικές

ή φιλοσοφικές πεποιθήσεις, θέματα υγείας, κοινωνικής πρόνοιας, συνδικαλιστικής δράσης, ποινικού μητρώου ή ερωτικής ζωής. [10]

2.4 Πολιτικές Ιδιωτικότητας στις Εφαρμογές

Τα έξυπνα τηλέφωνα, με τις πολυπληθείς λειτουργίες τους, αλλά και τις εκατομμύρια διαθέσιμες εφαρμογές προς χρήση, φιλοξενούν πληθώρα ετερογενών δεδομένων και διαθέτουν μια μεγάλη συλλογή προσωπικών στοιχείων για τον κάθε χρήστη. Έχοντας πλέον διεισδύσει στην καθημερινότητα μας, εμπλέκονται σε αυτήν αλλά και στην ιδιωτικότητα μας. Γι' αυτό το λόγο κάθε εφαρμογή και ιστοσελίδα οφείλει να παρουσιάζει στους χρήστες τα στοιχεία που συλλέγει από αυτούς αλλά και το σκοπό χρήσης τους. Αυτά διατυπώνονται υπό την μορφή **Πολιτικών Ιδιωτικότητας**, οι οποίες μπορεί να βρίσκονται είτε υπό μορφή φυσικής γλώσσας διαθέσιμες στην εφαρμογή ή ιστοσελίδα, είτε υπό τη μορφή xml γλώσσας, οι οποίες γίνονται κατανοητές από προγράμματα λογισμικού. Η πιο γνωστή πλατφόρμα για την κωδικοποίηση των πολιτικών είναι η P3P (Platform for Privacy Preferences). Παρουσιάστηκε το 1997 και παρέχει σε ιστοσελίδες τη δυνατότητα να κωδικοποιούν τις πολιτικές ιδιωτικότητας τους και τις κινήσεις τους αναφορικά με τη συλλογή και επεξεργασία των δεδομένων των χρηστών σε xml γλώσσα. Έτσι, παρέχεται η δυνατότητα στους ειδικούς, να ερμηνεύσουν τις πολιτικές ιδιωτικότητας και να κρίνουν εάν είναι επαρκείς ανάλογα με τις επιθυμίες του χρήστη. [11]

Εταιρεία	Περιγραφή Παραβίασης	Πηγή
Ebay	Κλοπή βάσης δεδομένων με συνθηματικά και προσωπικά στοιχεία χρηστών. Οι χρήστες ειδοποιήθηκαν για να αλλάξουν τα συνθηματικά τους	Ανακοίνωση της εταιρίας Ebay
Adobe	Κλοπή πηγαίου κώδικα λογισμικού, βάσης δεδομένων με συνθηματικά, προσωπικά στοιχεία και κρυπτογραφημένους αριθμούς πιστωτικών καρτών από 2,9 εκατ. χρήστες.	Ανακοίνωση του υπευθύνου ασφαλείας της Adobe
Sony	Κλοπή στοιχείων που αφορούσαν υπαλλήλους της Sony, αλλά και αντίγραφα μη προβεβλημένων ταινιών.	Wikipedia
Home Depot	Κλοπή στοιχείων πιστωτικών καρτών.	Ανακοίνωση της εταιρίας Home Depot

Πίνακας 4. Ενδεικτικές περιπτώσεις παραβίασης της ασφάλειας χρηστών σε σύγχρονα πληροφοριακά συστήματα [12]

Τον Αύγουστο του 2014, περισσότερες από 500 προσωπικές φωτογραφίες διάσημων αναρτήθηκαν ανώνυμα στην ιστοσελίδα 4chan, στην οποία ο καθένας μπορεί να ανεβάσει ότι επιθυμεί χωρίς εγγραφή. Το υλικό αυτό, ήταν αποθηκευμένο στο iCloud της εταιρίας Apple, και κυκλοφόρησε πολύ γρήγορα σε όλα τα κοινωνικά δίκτυα. Η δήλωση της Apple, ήταν πως το σύστημα παραβιάστηκε από στοχευμένη επίθεση στα συνθηματικά και στις “ερωτήσεις ασφαλείας” των χρηστών.

Ακόμα ένα γεγονός που συνέβαλε σε μεγάλο βαθμό στη συνειδητοποίηση των δυνατοτήτων μαζικής παρακολούθησης, συλλογής και επεξεργασίας τεράστιου όγκου προσωπικών δεδομένων ήταν η αποκάλυψη του Edward Snowden το 2013, ενός εργαζόμενου μιας ιδιωτικής εταιρείας, ο οποίος έφερε στο φως της δημοσιότητας χιλιάδες απόρρητα έγγραφα που παρουσιάζουν τις δυνατότητες παρακολούθησης της NSA(National Security Agency). [\[12\]](#)

Ανησυχία είχε προκαλέσει επίσης, η υπεξαίρεση προσωπικών στοιχείων από την εταιρεία συλλογής δεδομένων Cambridge Analytica το 2014. Όπως αναφέρουν οι New York Times, προσωπικά στοιχεία 50 εκατομμυρίων χρηστών του Facebook πάρθηκαν με στόχο την ενίσχυση της υποψηφιότητας του D.Trump έναντι αυτή της H.Clinton. Η ομάδα του Trump πραγματοποιούσε profiling, για να εντοπίζει υποψήφιους ψηφοφόρους έτσι ώστε να τους βομβαρδίζει με διαφημίσεις υπέρ της υποψηφιότητας Trump. Το Facebook διέκοψε κάθε συνεργασία με την εν λόγω εταιρεία. Ακόμα ένα παράδειγμα υποκλοπής προσωπικών στοιχείων αποτελεί η επίθεση στην Αγγλική τράπεζα Tesco όπου 9.000 τραπεζικοί λογαριασμοί χρηστών παραβιάστηκαν καθώς και δύομισι εκατομμύρια λίρες κλάπηκαν. [\[13\]](#)

Τα στοιχεία αυτά, αποτελούν ένα μικρό δείγμα παραδειγμάτων παραβίασης απόρρητων στοιχείων, όμως αρκούν για να φτάσουμε στο συμπέρασμα ότι η σημασία του ζητήματος της διαφύλαξης των προσωπικών δεδομένων και της προστασίας της ιδιωτικότητας δεν χρήζει απόδειξης.

Σύμφωνα με έρευνα που έλαβε χώρα στις Η.Π.Α, το 91% των ιστοσελίδων και εφαρμογών συλλέγουν προσωπικές πληροφορίες και το 90% προσωπικά δεδομένα αναγνώρισης. Παράλληλα οι Hochhauser (2001), Antón (2004), McDonald (2009) και (Singh et al. 2011) υποστηρίζουν ότι οι χρήστες χρειάζονται υψηλότερο από το μέσο επίπεδο ανάγνωσης και ορθογραφίας για να κατανοήσουν τους νομικούς όρους που χρησιμοποιούνται στις πολιτικές ιδιωτικότητας ενώ σύμφωνα με τους (Milne and Culnan 2004), αυτός είναι και ο λόγος που οι χρήστες δείχνουν ελάχιστο ενδιαφέρον για να τις διαβάσουν . [\[14\]](#)

3. Μοντέλα Αδειών Πρόσβασης

3.1 Android και Άδειες Πρόσβασης

Η διαφύλαξη των προσωπικών δεδομένων των χρηστών είναι αναγκαία και γι' αυτό το λόγο όλες οι εφαρμογές Android υποχρεούνται να δηλώνουν με ακρίβεια τις άδειες που ζητούν αλλά και το σκοπό χρήσης τους. Οι άδειες αποτελούν ουσιαστικά μια μορφή δήλωσης, σχετικά με την πρόσβαση που επιθυμεί να αποκτήσει η εκάστοτε εγκατεστημένη εφαρμογή μέσα στο λειτουργικό σύστημα της συσκευής.

Το Android χρησιμοποιεί τον μηχανισμό αδειών προσπέλασης του λειτουργικού συστήματος Linux, εφαρμόζοντας διαχωρισμό προνομίων, όπου κάθε εφαρμογή τρέχει με μια ξεχωριστή ταυτότητα συστήματος. Έτσι, οι εφαρμογές είναι διαχωρισμένες και απομονωμένες η μια από την άλλη, αλλά και από το σύστημα. Το Android δίνει σε κάθε εφαρμογή ένα μοναδικό αναγνωριστικό χρήστη ή αλλιώς UID και η εφαρμογή τρέχει ως ξεχωριστή διεργασία. Μόνο οι διεργασίες με το ίδιο αναγνωριστικό χρήστη θα μπορούν να μοιράζονται τους ίδιους πόρους της συσκευής και αφού κάθε εφαρμογή έχει το δικό της αναγνωριστικό, καμία εφαρμογή δεν έχει πρόσβαση σε ίδιους πόρους με κάποια άλλη.

3.2 Επίπεδα Προστασίας των Αδειών Πρόσβασης

Οι άδειες πρόσβασης χωρίζονται σε τρία επιμέρους επίπεδα προστασίας.

- ❖ **Κανονικές άδειες (normal):** Οι κανονικές άδειες καλύπτουν περιοχές στις οποίες η εφαρμογή χρειάζεται άδεια πρόσβασης σε δεδομένα ή πόρους του συστήματος έξω από το περιβάλλον λειτουργίας της (sandbox), αλλά σε σημεία όπου είναι πολύ μικρός ο κίνδυνος για τα προσωπικά δεδομένα του χρήστη ή τη λειτουργία των υπόλοιπων εφαρμογών. Ένα παράδειγμα τέτοιας άδειας είναι αυτή της ρύθμισης της ζώνης ώρας. Αν μια εφαρμογή χρειάζεται αυτήν την άδεια, αυτόματα το σύστημα εγκρίνει την πρόσβαση στην εφαρμογή.
- ❖ **Επικίνδυνες άδειες (dangerous):** Οι επικίνδυνες άδειες καλύπτουν περιοχές όπου η εφαρμογή ζητάει άδεια πρόσβασης σε δεδομένα ή πόρους του συστήματος, τα οποία περιλαμβάνουν προσωπικά δεδομένα του χρήστη, ή θα μπορούσαν να επηρεάσουν αποθηκευμένα δεδομένα ή τη λειτουργία των υπόλοιπων εφαρμογών. Αν μια εφαρμογή δηλώνει ότι χρειάζεται να της

χορηγηθεί μια επικίνδυνη άδεια, τότε ο χρήστης θα πρέπει ρητά να της χορηγήσει την άδεια.

- ❖ **Άδειες με Υπογραφή:** Πρόκειται για άδειες πρόσβασης, οι οποίες χορηγούνται αν η εφαρμογή που απαιτείται άδεια, υπογραφεί με το ίδιο πιστοποιητικό με την εφαρμογή που ορίζει την άδεια υπογραφής.

ACCESS_LOCATION_EXTRA_COMMANDS
ACCESS_NETWORK_STATE
ACCESS_NOTIFICATION_POLICY
ACCESS_WIFI_STATE
BLUETOOTH
BLUETOOTH_ADMIN
BROADCAST_STICKY
CHANGE_NETWORK_STATE
CHANGE_WIFI_MULTICAST_STATE
CHANGE_WIFI_STATE
DISABLE_KEYGUARD
EXPAND_STATUS_BAR
FOREGROUND_SERVICE
GET_PACKAGE_SIZE
INSTALL_SHORTCUT
INTERNET
KILL_BACKGROUND_PROCESSES
MANAGE_OWN_CALLS
MODIFY_AUDIO_SETTINGS

NFC
READ_SYNC_SETTINGS
READ_SYNC_STATS
RECEIVE_BOOT_COMPLETED
REORDER_TASKS
REQUEST_COMPANION_RUN_IN_BACKGROUND
REQUEST_DELETE_PACKAGES
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
SET_ALARM
SET_WALLPAPER
SET_WALLPAPER_HINTS
TRANSMIT_IR
USE_FINGERPRINT
VIBRATE
WAKE_LOCK
WRITE_SYNC_SETTINGS

Πίνακας 5. Κανονικές άδειες [\[15\]](#)

ΟΜΑΔΑ ΑΔΕΙΩΝ (PERMISSION GROUPS)	ΑΔΕΙΑ(PERMISSION)
Ημερολόγιο	READ_CALENDAR, WRITE_CALENDAR
Κάμερα	CAMERA
Επαφές	READ_CONTACTS, WRITE_CONTACTS, GET_ACCOUNTS
Τοποθεσία	ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION
Μικρόφωνο	RECORD_AUDIO
Τηλέφωνο	READ_PHONE_STATE, CALL_PHONE, READ_CALL_LOG, WRITE_CALL_LOG, ADD_VOICEMAIL, USE_SIP, PROCESS_OUTGOING_CALLS
Αισθητήρες	BODY_SENSORS
SMS	SEND_SMS, RECEIVE_SMS, READ_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS
Αποθήκευση	READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE

Πίνακας 6. Επικίνδυνες άδειες και ομάδες αδειών [\[16\]](#)

BIND_ACCESSIBILITY_SERVICE
BIND_AUTOFILL_SERVICE
BIND_CARRIER_SERVICES
BIND_CHOOSER_TARGET_SERVICE
BIND_CONDITION_PROVIDER_SERVICE
BIND_DEVICE_ADMIN
BIND_DREAM_SERVICE
BIND_INCALL_SERVICE
BIND_INPUT_METHOD
BIND_MIDI_DEVICE_SERVICE
BIND_NFC_SERVICE
BIND_NOTIFICATION_LISTENER_SERVICE
BIND_PRINT_SERVICE
BIND_SCREENING_SERVICE
BIND_TELECOM_CONNECTION_SERVICE
BIND_TEXT_SERVICE
BIND_TV_INPUT
BIND_VISUAL_VOICEMAIL_SERVICE
BIND_VOICE_INTERACTION

BIND_VPN_SERVICE
BIND_VR_LISTENER_SERVICE
BIND_WALLPAPER
CLEAR_APP_CACHE
MANAGE_DOCUMENTS
READ_VOICEMAIL
REQUEST_INSTALL_PACKAGES
SYSTEM_ALERT_WINDOW
WRITE_SETTINGS
WRITE_VOICEMAIL

Πίνακας 7. Άδειες με υπογραφή
[\[16\]](#)

3.3 Οι Αλλαγές στο Marshmallow Android 6.0

Οι εφαρμογές δεν έχουν άμεση πρόσβαση στους πόρους της συσκευής, τρέχουν μόνες τους για λόγους ασφαλείας. Έτσι, κάθε λειτουργικό σύστημα διαθέτει άδειες πρόσβασης οι οποίες παραχωρούν πρόσβαση στον προγραμματιστή σε επιμέρους πόρους, όπως στις επαφές ή στην κάμερα με σκοπό την αξιοποίηση τους μέσα στην εφαρμογή.

Πριν τις αλλαγές που επέφερε η έκδοση Android 6.0, η πρόσβαση στα δικαιώματα των εφαρμογών απαιτούσε root στην συσκευή. Οι άδειες των εφαρμογών δινόταν ως προεπιλογή κατά την εγκατάσταση της εφαρμογής, και ο χρήστης δεν είχε τρόπο να αρνηθεί κάποιες ή όλες τις άδειες, η μόνη επιλογή που είχε ήταν να μην εγκαταστήσει την εφαρμογή.

Με την έκδοση Android 6.0 ο χρήστης επιλέγει ποια δικαιώματα θέλει να παραχωρήσει μετά την εγκατάσταση της εφαρμογής, και όχι πριν από την εγκατάσταση όπως ίσχυε στις προηγούμενες εκδόσεις. Ο χρήστης νιώθει μεγαλύτερη προστασία, καθώς επιλέγει μια προς μια, ποια άδεια θέλει να εγκρίνει. Επιπλέον, ο χρήστης έχει τη δυνατότητα εάν αλλάξει γνώμη ως προς την αποδοχή μιας άδειας να ανατρέξει στις ρυθμίσεις και να την τροποποιήσει. Όπως είναι φυσικό, η ενέργεια αυτή μπορεί να εμποδίσει κάποιες από τις λειτουργίες της εφαρμογής. Για παράδειγμα αν ο χρήστης δεν παραχωρήσει άδεια για την κάμερα της συσκευής αλλά προσπαθήσει να κάνει βίντεο κλήση, η λειτουργία δεν θα πραγματοποιηθεί.

Είναι εμφανές ότι με τις αλλαγές που επέφερε το Android 6.0, ο χρήστης νιώθει μεγαλύτερη προστασία, όμως υπάρχει ένα σημείο το οποίο μπορεί ακόμα να αποτελέσει απειλή για την ιδιωτικότητα του. Το Google Play κατηγοριοποιεί τις άδειες σε ομάδες σχετικών αδειών. Έτσι, παίρνοντας ως παράδειγμα το δικαίωμα μιας εφαρμογής στην ανάγνωση επαφών, ζητείται από το χρήστη η άδεια `READ_CONTACTS`. Όταν όμως ο χρήστης εγκαταστήσει την εφαρμογή θα αντιληφθεί πως ζητείται άδεια για όλη την ομάδα αδειών που αφορούν τις επαφές. Αν λοιπόν ο χρήστης χορηγήσει την άδεια αυτή, θα χορηγήσει παράλληλα και όλες τις σχετικές άδειες, στο παράδειγμα μας, την `WRITE_CONTACTS` και `GET_ACCOUNTS`. Συγχρόνως, η εφαρμογή αυτή σε επόμενη αναβάθμιση της, εάν προσθέσει καινούργιες άδειες στην ομάδα αδειών, δεν θα ζητήσει ξανά παραχώρηση άδειας από το χρήστη, καθώς την είχε χορηγήσει σε προηγούμενη αναβάθμιση, και πιθανότατα ο χρήστης να μην γνωρίζει για την προσθήκη αυτή. [\[17\]](#)

Παράλληλα, το Google Play απειλεί την ιδιωτικότητα του χρήστη με τον τρόπο ομαδοποίησης των αδειών. Πολύ ευαίσθητα προσωπικά δεδομένα ομαδοποιούνται μαζί με λιγότερο σημαντικά στοιχεία του χρήστη. Μια πολύ σημαντική άδεια, η οποία γίνεται εμφανής σε πολλές εφαρμογές, είναι η `READ_PHONE_STATE`. Με την άδεια αυτή η εφαρμογή μπορεί να πάρει πληροφορίες για την κατάσταση της συσκευής για παράδειγμα αν βρίσκεται σε κλήση, αν η συσκευή είναι ανοικτή ή κλειστή. Παράλληλα όμως με την ίδια άδεια μπορούν να αντληθούν σημαντικά προσωπικά και μοναδικά στοιχεία του χρήστη όπως το IMEI (μοναδική ταυτότητα κάθε συσκευής), το IMSI (μοναδικό χαρακτηριστικό

κάθε συνδρομητή αλλά και πληροφορίες για τη χώρα του χρήστη, το ICCID (σειριακό αριθμό της κάρτας SIM) καθώς και αρχεία κλήσεων . Σε εφαρμογές οι οποίες υποστηρίζουν παλαιότερες εκδόσεις Android, η άδεια αυτή ζητείται από το χρήστη ακόμα και αν δεν την χρειάζονται, καθώς στις παλαιότερες εκδόσεις χορηγούνταν από προεπιλογή.

Αυτά τα κενά στις άδειες πρόσβασης εντείνουν όλο και περισσότερο την ανησυχία των χρηστών ως προς την προστασία των προσωπικών τους δεδομένων και της ιδιωτικότητάς τους.

3.4 Μειονεκτήματα των Αδειών Πρόσβασης στο Android

Όπως αναφέρθηκε στο αμέσως προηγούμενο κεφάλαιο, τα μοντέλα αδειών πρόσβασης των τωρινών λειτουργικών συστημάτων κρίνονται, βάσει νόμων, ανεπαρκή όσον αφορά τη διαφύλαξη της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων των χρηστών.

Η ανεπάρκεια αυτή, φαίνεται από τα τρία παρακάτω πιο σημαντικά μειονεκτήματα των αδειών πρόσβασης στο Android :

- ❖ Πριν το Android 6, ο χρήστης δέχεται όλες τις άδειες που η εφαρμογή του ζητάει, αλλιώς ο ίδιος δεν μπορεί να εγκαταστήσει την εφαρμογή. Ο χρήστης δεν μπορούσε να προβεί σε κάποια διαπραγμάτευση των επιλογών πρόσβασης και χρήσης. Έτσι, αν υποθετικά μια εφαρμογή κοινωνικής δικτύωσης, εκτός από τις βασικές άδειες που σχετίζονται με τη λειτουργικότητα της, ζητήσει για παράδειγμα πρόσβαση στα SMS της συσκευής, ο χρήστης δεν μπορεί να το αποτρέψει. Ευτυχώς, στο Android 6 αυτό άλλαξε προς τη θετική, για τους χρήστες, πλευρά. Παράλληλα όμως, αν μια εφαρμογή έχει σχεδιαστεί για παλαιότερη έκδοση Android, αυτή δεν θα ζητήσει κάποια συγκατάθεση από το χρήστη, αλλά θα πάρει αυθαίρετα πρόσβαση σε κάθε πόρο της συσκευής. Ο μόνος τρόπος να το αλλάξει αυτό ο χρήστης, είναι ανατρέχοντας στην ρυθμίσεις χειροκίνητα.
- ❖ Όπως αναφέραμε και σε προηγούμενο κεφάλαιο, η μεγαλύτερη ανησυχία των χρηστών αποτελεί η αλόγιστη συλλογή των προσωπικών τους δεδομένων χωρίς τη γνωστοποίηση του σκοπού χρήσης τους, από τις εφαρμογές. Το πιο σημαντικό δικαίωμα του χρήστη το οποίο είναι η *Αρχή του Προσδιορισμού του Σκοπού*, παραβιάζεται από το μεγαλύτερο ποσοστό των εφαρμογών του Android, αφού οι εφαρμογές συλλέγουν τεράστιους όγκους προσωπικών δεδομένων των χρηστών τους, χωρίς να κάνουν γνωστή την ανάγκη συλλογής αυτών.

- ❖ Ένα από τα πιο σημαντικά μειονεκτήματα των εφαρμογών Android αποτελεί το δικαίωμα μιας εφαρμογής να μεταδώσει προσωπικά δεδομένα σε τρίτες οντότητες. Ο χρήστης συμφωνεί στην παραχώρηση κάποιων ή όλων των αδειών όμως δεν γνωρίζει αν τα στοιχεία του χρησιμοποιούνται από την εκάστοτε εφαρμογή και μόνο, ή αν διακινούνται εκτός συσκευής για διαφημιστικούς, εμπορικούς ή άλλους λόγους. Ο σκοπός αυτός πρέπει να δηλώνεται ρητά από τις εφαρμογές στις πολιτικές ιδιωτικότητας τους, παρ' όλα αυτά είναι κάτι που οι περισσότερες εφαρμογές επιλέγουν να μην αναφέρουν ξεκάθαρα. [\[18\]](#)

4. Μεθοδολογία Εργασίας

4.1 Υλοποίηση

Επ' αφορμή της παρούσας πτυχιακής εργασίας υλοποιήθηκε προγραμματιστικό κομμάτι κώδικα σε γλώσσα προγραμματισμού c# με το οποίο αντλήθηκαν τα δεδομένα για κάθε εφαρμογή ορισμένων κατηγοριών του Google Play. Οι εφαρμογές οι οποίες αντλήθηκαν από το Google Play Store αγγίζουν σε αριθμό τις 3026, δείγμα αρκετά ικανοποιητικό για την εξαγωγή εμπεριστατωμένων συμπερασμάτων.

Οι κατηγορίες του Play Store από τις οποίες αντλήθηκαν τα δεδομένα αριθμούνται στις 32 και είναι οι εξής :

General:

- | | |
|---------------------|---------------------|
| • Art & Design | • Lifestyle |
| • Auto & Vehicles | • Maps & Navigation |
| • Beauty | • Medical |
| • Books & Reference | • Music & Audio |
| • Business | • News & Magazines |
| • Comics | • Parenting |
| • Communication | • Personalization |
| • Dating | • Photography |
| • Education | • Productivity |
| • Entertainment | • Shopping |
| • Events | • Social |
| • Finance | • Sports |
| • Food & Drink | • Tools |
| • Health & Fitness | • Travel & Local |
| • House & Home | • Weather |
| • Libraries & Demo | • Family |

Μέσω του κώδικα, αντλήθηκαν οι εξής πληροφορίες για κάθε εφαρμογή :

- ❖ Όνομα εφαρμογής
- ❖ URL εφαρμογής
- ❖ Άδειες που ζητά η κάθε εφαρμογή από το χρήστη

Τα δεδομένα αυτά στη συνέχεια, καταχωρήθηκαν σε μια βάση δεδομένων, η οποία δημιουργήθηκε στα πλαίσια της παρούσας εργασίας, σε ένα ανοικτού κώδικα λογισμικό (open source), το sqlite.

Οι πληροφορίες καταχωρήθηκαν σε πέντε διαφορετικούς πίνακες με σκοπό τη δημιουργία και εκτέλεση συγκεκριμένων ερωτημάτων (Queries) έτσι ώστε να καταλήξουμε σε αποτελέσματα και στη συνέχεια συμπεράσματα όσον αφορά τα δικαιώματα που ζητούν οι δημιουργοί των εφαρμογών από τους χρήστες. Για παράδειγμα, πόσα δικαιώματα ζητά μια εφαρμογή από το χρήστη; πόσες και ποιες είναι οι εφαρμογές που ζητούν τα περισσότερα δικαιώματα;

Τα ήδη υπάρχοντα APIs που ήταν διατεθειμένα στο διαδίκτυο δεν ήταν κατάλληλα καθώς είτε ήταν πολύ παλιά και άρα δεν εμπεριείχαν χαρακτηριστικά που η Google έχει προσθέσει πρόσφατα στο Play Store, είτε δεν υποστήριζαν την άντληση των αδειών πρόσβασης που εμείς επιθυμούσαμε. Γι' αυτούς τους λόγους η συγγραφέας υλοποίησε το απαραίτητο κομμάτι κώδικα με το οποίο και αντλήθηκαν τα απαραίτητα δεδομένα.

Μολονότι στο Play Store υπάρχουν διαθέσιμες Android εφαρμογές ακριβώς γι' αυτόν τον σκοπό, δηλαδή την άντληση των αδειών πρόσβασης μιας εφαρμογής, κάτι τέτοιο δεν είναι λειτουργικό καθώς θα έπρεπε να κατεβάσουμε για κάθε εφαρμογή χειροκίνητα όλες τις άδειες της και αυτό αποτελεί μια χρονοβόρα διαδικασία. Τέλος, οι εφαρμογές θα παρείχαν τις πληροφορίες που θα ήταν διαθέσιμες για τη χώρα στην οποία ανήκει ο χρήστης, όμως δεν θα μπορούσαμε να συλλέξουμε πληροφορίες για την ίδια εφαρμογή αλλά για διαφορετική χώρα.

4.2 Εργαλεία

Για την πραγματοποίηση του προγραμματιστικού μέρους της πτυχιακής εργασίας, την καταχώρηση των αδειών πρόσβασης των εφαρμογών αλλά και την εξαγωγή συμπερασμάτων με βάσεις αυτές, χρησιμοποιήθηκαν τα εξής εργαλεία :

- ❖ Η **γλώσσα προγραμματισμού C#** : Η συγκεκριμένη γλώσσα προγραμματισμού χρησιμοποιήθηκε στην παρούσα εργασία για αρκετούς λόγους. Η C# δημιουργήθηκε από την Microsoft και αποτελεί μια από τις πιο διάσημες αντικειμενοστραφείς γλώσσες στο χώρο του προγραμματισμού. Είναι σχετικά απλή στη σύνταξη της και το διαδίκτυο διαθέτει μεγάλο όγκο βοηθητικού υλικού για τους χρήστες της. Συνεπώς, η απλότητα της γλώσσας σε συνδυασμό με την εμπειρία της συγγραφέα στη συγκεκριμένη γλώσσα, βοήθησε τη συγγραφή του προγραμματιστικού μέρους της εργασίας.

Η τελευταία και πιο πρόσφατη έκδοση της C# είναι η έκδοση 5.0 η οποία κυκλοφόρησε τον Αύγουστο του 2012.

Ο κώδικας γράφτηκε σε IDE περιβάλλον **Visual Studio 2019** και **.NET Framework 4.5**.

- **Visual Studio 2019:** Αποτελεί ένα ολοκληρωμένο προγραμματιστικό περιβάλλον ανάπτυξης από την Microsoft. Χρησιμοποιείται για την ανάπτυξη προγραμμάτων, ιστοσελίδων, εφαρμογών ιστού αλλά και εφαρμογές κινητών. Το Visual Studio διαθέτει ένα άριστο ενσωματωμένο πρόγραμμα εντοπισμού σφαλμάτων (debugger) καθώς και επεξεργαστή κώδικα (code editor), εργαλεία που αποτελούν τον κυριότερο λόγο επιλογής του Visual Studio από τους προγραμματιστές αφού παρέχουν ευκολία και ταχύτητα. Επιπλέον, το Visual Studio υποστηρίζει περισσότερες από 36 γλώσσες προγραμματισμού όπως C, C#, C++, Visual Basic, JavaScript, XML, HTML, CSS κ.α. [\[19\]](#)
- **.NET Framework 4.5:** Αποτελεί ένα πλαίσιο λογισμικού το οποίο έχει δημιουργηθεί από την Microsoft και εκτελείται κυρίως στα Windows. Το πλαίσιο αυτό περιέχει μια μεγάλη βιβλιοθήκη κλάσεων όπου ονομάζεται Framework Class Library (FCL). Η βιβλιοθήκη αυτή παρέχει δια λειτουργικότητα (interoperability) μεταξύ διαφορετικών γλωσσών προγραμματισμού δηλαδή κάθε γλώσσα μπορεί να χρησιμοποιήσει τον κώδικα μιας άλλης γλώσσας. Τα προγράμματα που έχουν γραφτεί για το .NET Framework εκτελούνται σε περιβάλλον λογισμικού το οποίο ονομάζεται Common Language Runtime (CLR). Αποτελεί μια εικονική μηχανή εφαρμογών (Virtual Machine) και παρέχει ασφάλεια, διαχείριση μνήμης αλλά και χειρισμό εξαιρέσεων. Συνοψίζοντας, η βιβλιοθήκη FCL και η εικονική μηχανή CLR αποτελούν το γνωστό πλαίσιο λογισμικού .NET Framework. Η έκδοση που χρησιμοποιήθηκε στην παρούσα πτυχιακή είναι η έκδοση 4.5.

Στο προγραμματιστικό κομμάτι επίσης, χρησιμοποιήθηκαν τριτες βιβλιοθήκες οι οποίες δεν ανήκουν στις βιβλιοθήκες του Visual Studio :

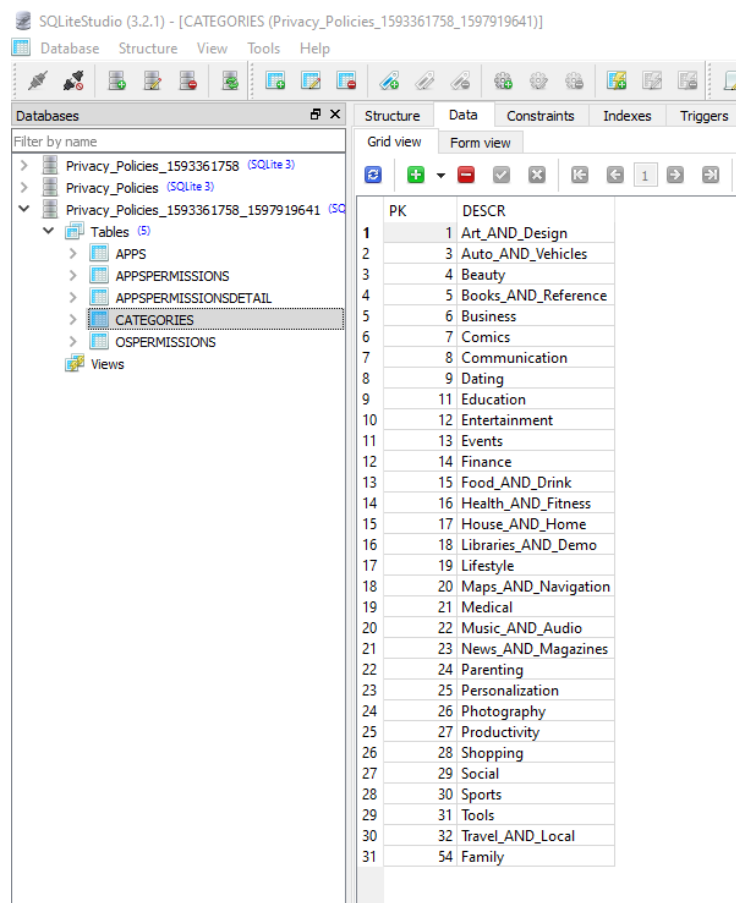
- **Webdriver API Selenium:** Στην παρούσα πτυχιακή χρησιμοποιήθηκε η 3.141.0 version του Webdriver Selenium και αποτελεί ένα plugin εργαλείο της Google το οποίο εξομοιώνει την πλοήγηση, που θα κάναμε ως χρήστες με το ποντίκι σε μια ιστοσελίδα, με κώδικα. Η βιβλιοθήκη Selenium δέχεται εντολές, τις οποίες και στέλνει στο πρόγραμμα περιήγησης και στη συνέχεια ανακτά τα επιθυμητά αποτελέσματα.
- **Html Agility Pack:** Αποτελεί μια βιβλιοθήκη η οποία χρησιμοποιείται στη γλώσσα C# και είναι μια τεχνική με την

οποία ο προγραμματιστής μπορεί να αντλήσει δεδομένα από μια ιστοσελίδα. Η Html Agility Pack ουσιαστικά είναι ένας αναλυτής ο οποίος διαβάζει κείμενο σε XML και το μετατρέπει σε Object, δηλαδή σε ένα αντικείμενο με συγκεκριμένες ιδιότητες.

- **Newtonsoft Json** : Μια ακόμη βιβλιοθήκη, η οποία λειτουργεί και αυτή ως αναλυτής, αφού διαβάζει κείμενο Json και το μετατρέπει σε Object, δηλαδή σε ένα αντικείμενο με συγκεκριμένες ιδιότητες.

❖ **Η βάση δεδομένων Sqlite** : Η sqlite αποτελεί ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων, είναι ανοικτού κώδικα (open source), γρήγορη και εύκολη στη χρήση. Τα δεδομένα των εφαρμογών που αντλήθηκαν με τη βοήθεια του προγράμματος, καταχωρήθηκαν σε μια βάση δεδομένων sqlite.

Όπως φαίνεται και από την παρακάτω εικόνα, οι πίνακες που δημιουργήθηκαν με βάση τα δεδομένα που αντλήθηκαν από τις εφαρμογές του Play Store είναι οι εξής:



Εικόνα 1. Οι πίνακες της βάσης δεδομένων.

Ο κάθε ένας από αυτούς τους πίνακες περιέχει χρήσιμα δεδομένα, τα οποία αντλήθηκαν από την ιστοσελίδα του Play Store, με τη χρήση των οποίων θα δημιουργηθούν και θα τρέξουν ορισμένα

queries για να καταλήξουμε σε συμπεράσματα αναφορικά με τις άδειες πρόσβασης των εφαρμογών.

Η βάση δεδομένων αποτελείται από τους εξής πίνακες :

❖ **APPS:** Ο πίνακας αυτός περιέχει όλες τις βασικές πληροφορίες των εφαρμογών που αντλήθηκαν από το Play Store. Για κάθε μια απ' αυτές περιέχει :

- το Primary Key (**PK**) της κάθε εφαρμογής,
- το όνομα της (**DESCR**),
- την εταιρεία που την δημιούργησε (**COMPANY**),
- την κατηγορία της στο Play Store (**CATDESCR**),
- τον αριθμό της κατηγορίας (**CATEGORIES**),
- καθώς και το url της (**URLREF**).

PK	DESCR	COMPANY	CATDESCR	CATEGORIES	URLREF
1	iis Paint X	iis inc.	Art_AND_Design	1	https://play.google.com/st
2	Art Camera - Cartoon Pencil Sketch Art Effect Photo	Model X Apps	Art_AND_Design	1	https://play.google.com/st
3	Poster Maker Flyer Maker 2020 free Ads Page Design	Splendid App Maker	Art_AND_Design	1	https://play.google.com/st
4	Floor Plan Creator	Marcin Lewandowski	Art_AND_Design	1	https://play.google.com/st
5	Posters: Story Editor template design post	KVADGroup App Studio	Art_AND_Design	1	https://play.google.com/st
6	T-Shirt Design - Custom T Shirts	Pickles Fox	Art_AND_Design	1	https://play.google.com/st
7	Tattoo Font Designer - A tattoo lettering app	Evil ink - Tattoo Design Apps and Calligraphy fonts	Art_AND_Design	1	https://play.google.com/st
8	Logo Maker - Logo Creator, Generator & Designer	AR Tech	Art_AND_Design	1	https://play.google.com/st
9	SketchBook - draw, sketch & paint	SketchBook	Art_AND_Design	1	https://play.google.com/st
10	MediBang Paint - Make Art!	MediBang Inc.	Art_AND_Design	1	https://play.google.com/st
11	শিখন - লিখন - বাংলা - Bangla on Photos	Shajid Hasan	Art_AND_Design	1	https://play.google.com/st
12	Drawing - Sketch	yys	Art_AND_Design	1	https://play.google.com/st
13	Colorify - Drawing & Coloring	Creative APPS	Art_AND_Design	1	https://play.google.com/st
14	Smoke Name Art - Smoky Effect Focus n Filter Maker	AppX Studio	Art_AND_Design	1	https://play.google.com/st
15	TextArt★ Cool Text creator	Quarzo Apps	Art_AND_Design	1	https://play.google.com/st
16	Logo Maker 2020- Logo Creator, Logo Design	Quantum Appx	Art_AND_Design	1	https://play.google.com/st
17	Best Free Fire wallpaper HD new	Unsei Dev	Art_AND_Design	1	https://play.google.com/st
18	How to Draw Graffiti - Name Creator	Sweetfit Studios	Art_AND_Design	1	https://play.google.com/st
19	Social Media Post Maker - Social Post	stylish app world	Art_AND_Design	1	https://play.google.com/st
20	عبارات فنانة جاهزة للتصميم	مودو العربي Modu Arabi	Art_AND_Design	1	https://play.google.com/st
21	Kawaii Wallpapers Cute Backgrounds	SandStorm Studios	Art_AND_Design	1	https://play.google.com/st
22	My Name in 3D Live Wallpaper	My Name Cube Apps	Art_AND_Design	1	https://play.google.com/st
23	ملك البلات	AppsTeam	Art_AND_Design	1	https://play.google.com/st
24	كلمات متنوعة وملصقات	مودو العربي Modu Arabi	Art_AND_Design	1	https://play.google.com/st
25	Urdu Poetry on Photo Urdu Shayri Status Maker	SHABIR	Art_AND_Design	1	https://play.google.com/st
26	Pixel Studio - Pixel art editor, GIF animation	Hippo	Art_AND_Design	1	https://play.google.com/st
27	Poster Maker, Flyer, Banner Maker, Graphic Design	postermakerflyerdesigner.com	Art_AND_Design	1	https://play.google.com/st
28	Rainbow Glitter Coloring Book - Unicorn Artist	Beansprites LLC	Art_AND_Design	1	https://play.google.com/st
29	SketchBook 2 - draw, sketch & paint	SketchBook	Art_AND_Design	1	https://play.google.com/st
30	CDRI(CoreDRAW) Viewer	V Vordl	Art_AND_Design	1	https://play.google.com/st
31	لؤلؤ Dolls Coloring game	happy time	Art_AND_Design	1	https://play.google.com/st
32	اسماء فنانة جاهزة للتصميم	مودو العربي Modu Arabi	Art_AND_Design	1	https://play.google.com/st
33	Adobe Spark Post: Graphic Design & Story Templates	Adobe	Art_AND_Design	1	https://play.google.com/st
34	Anime Wallpaper HD Anime List Wallpapers	SandStorm Studios	Art_AND_Design	1	https://play.google.com/st
35	Word Cloud	Smart Puffin	Art_AND_Design	1	https://play.google.com/st
36	Name Creator Fire-Free - FF NickFinder	Creator Tricks	Art_AND_Design	1	https://play.google.com/st
37	Sketch a Day: Daily challenges & tutorials	Tom Hicks	Art_AND_Design	1	https://play.google.com/st
38	Text Style, Text Art - Stylish Text - Fancy Text	OneDollar	Art_AND_Design	1	https://play.google.com/st
39	Wallpaper WINX Club	Zedev	Art_AND_Design	1	https://play.google.com/st
40	Stylish Name Maker - New Stylish name generator	AR Tech	Art_AND_Design	1	https://play.google.com/st
41	ملصقات وإنساب 2020 - WASTickerApps	Awson Apps	Art_AND_Design	1	https://play.google.com/st
42	Adobe Capture Vector & Pattern Maker	Adobe	Art_AND_Design	1	https://play.google.com/st
43	Behance: Photography, Graphic Design, Illustration	Adobe Inc.	Art_AND_Design	1	https://play.google.com/st
44	Concepts - Sketch, Design, Illustrate	TopHatch, Inc.	Art_AND_Design	1	https://play.google.com/st
45	Kids Paint	ng-labs	Art_AND_Design	1	https://play.google.com/st
46	মহেন্দ্র ডিজাইন মেহেন্দ্র - mehndi design 2020	ERT Apps	Art_AND_Design	1	https://play.google.com/st
47	Unicorn Art Pixel - Color By Number	Matthe S Thomas	Art_AND_Design	1	https://play.google.com/st

Εικόνα 2. Ο πίνακας Apps της βάσης δεδομένων.

❖ **APPSPERMISSIONS:** Ο πίνακας αυτός αφορά τις γενικές κατηγορίες των αδειών πρόσβασης και αποτελείται από τα εξής πεδία:

- Το Primary Key (**PK**),
- Τις κατηγορίες των αδειών πρόσβασης (**DESCR**),
- Την αντιστοιχία των αδειών πρόσβασης με τις άδειες του λειτουργικού συστήματος (**OSPERMISSIONS**).

- Το πεδίο **(CRUSIAL)** τύπου Boolean, που μας δείχνει αν η εκάστοτε ομάδα αδειών ανήκει στις επικίνδυνες άδειες (true or false).

The screenshot shows the SQLiteStudio interface with the APPSPERMISSIONS table selected. The table has two columns: APPSPERMISSIONS (INTEGER) and CRUSIAL (BOOLEAN). The data is as follows:

PK	DESCR	APPSPERMISSIONS	CRUSIAL
1	4 Photos/Media/Files	97,65,99,100	true
2	8 Identity	9,7,92	true
3	16 Access download manager.	89,170	true
4	18 Access all system downloads	89,170	true
5	26 Send download notifications.	89,170	true
6	31 Advanced download manager functions.	89,170	true
7	3 Wi-Fi connection information	8,60,61	false
8	34 Change WiMAX state	8,60,61	false
9	27 Access keyguard secure storage	69	true
10	32 Control displaying and hiding keyguard	69	false
11	28 Cellular data settings	63,132	true
12	1 Microphone	54,103,129	true
13	6 Camera	53	true
14	20 SMS	48,118,127,138,176	true
15	22 Wearable sensors/Activity data	45	true
16	24 Whitelist bluetooth device access.	42,3	true
17	11 Device ID & call information	23,27,67,159,11,25,51,52,95,106,108,168	true
18	7 Location	2,3,4,5,64,84,91	true
19	35 Google Maps	2,3	true
20	21 MMS Wakeup	128	true
21	25 Read email attachments	123	true
22	14 Device & app history	112,172	true
23	2 Storage	110,170	true
24	12 Phone	11,51,98,115,116	true
25	9 Contacts	109,169	true
26	13 Calendar	107,167	true
27	5 Other	NULL	NULL

Εικόνα 3. Ο πίνακας APPSPERMISSIONS της βάσης δεδομένων.

- ❖ **APPSPERMISSIONSDetail:** Ο πίνακας αυτός περιέχει με λεπτομέρεια όλες τις άδειες πρόσβασης που ζητούν οι εφαρμογές που κατεβάσαμε. Για παράδειγμα ο προηγούμενος πίνακας με όνομα **APPSPERMISSIONS** περιέχει την γενική άδεια πρόσβασης Contacts ενώ ο πίνακας **APPSPERMSSIONSDetails** διαθέτει λεπτομερής αναφορά των αδειών πρόσβασης που αφορούν την κατηγορία Contacts δηλαδή τις άδειες πρόσβασης Read your contacts και Find accounts on the device, όπως φαίνεται και στην παρακάτω εικόνα.

	PK	APPSPERMISSIONS	DESCR	APPS
1	1	1	read your contacts	1
2	2	1	find accounts on the device	1

Εικόνα 4. Οι επιμέρους άδειες πρόσβασης της κατηγορίας αδειών πρόσβασης Contacts.

Ο πίνακας **APPSPERMISSIONSDetail** λοιπόν, περιέχει τα εξής πεδία:

- Το Primary Key **(PK)**,
- Το πεδίο **(APPSPERMISSIONS)** που συσχετίζει αυτόν τον πίνακα με τον πίνακα των γενικών αδειών πρόσβασης,

- Τα ονόματα των λεπτομερών αδειών πρόσβασης (**DESCR**),
- Ο αριθμός της εφαρμογής που ζητά την εκάστοτε άδεια πρόσβασης με όνομα πεδίου (**APPS**),
- Και τέλος, την αντιστοιχία αυτών των αδειών πρόσβασης με αυτές του λειτουργικού συστήματος με όνομα πεδίου (**OSPERMISSION**).

SQLiteStudio (3.2.1) - [APPSPERMISSIONSDetail (Privacy_Policies_1593361758_1597919641)]

Database Structure View Tools Help

Databases

Filter by name

Privacy_Policies (SQLite 3)

Privacy_Policies_1593361758...

Tables (5)

APPS

APPSPERMISSIONS

APPSPERMISSIONSDetail

CATEGORIES

OSPERMISSIONS

Views

Grid view Form view

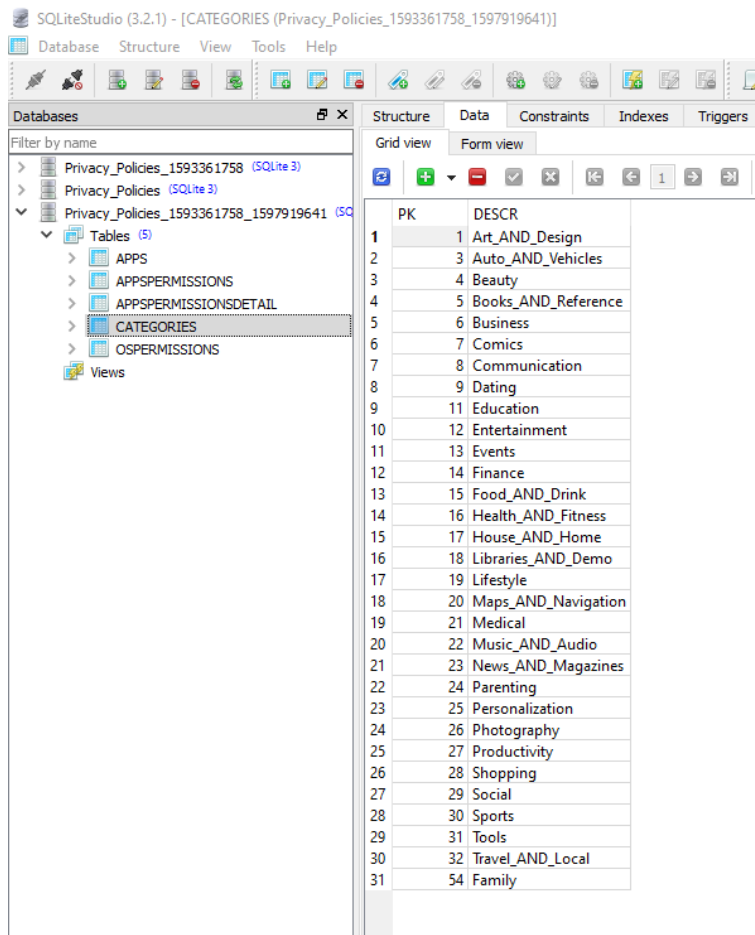
Filter data

Total rows loaded: 45967

PK	APPSPERMISSIONS	DESCR	APPS	OSPERMISSION
1	1	1 record audio	1	129
2	2	2 modify or delete the contents of your USB storage	1	110,170
3	3	2 read the contents of your USB storage	1	110
4	4	3 view Wi-Fi connections	1	8,60,61,13
5	5	4 modify or delete the contents of your USB storage	1	110,170
6	6	4 read the contents of your USB storage	1	110
7	7	5 receive data from Internet	1	8,89
8	8	5 control vibration	1	164
9	9	5 full network access	1	13,59
10	10	5 prevent device from sleeping	1	165
11	11	5 view network connections	1	8,60,61,13
12	12	4 read the contents of your USB storage	2	110
13	13	4 modify or delete the contents of your USB storage	2	110,170
14	14	2 read the contents of your USB storage	2	110
15	15	2 modify or delete the contents of your USB storage	2	110,170
16	16	6 take pictures and videos	2	55,56,97,54,103,129,53
17	17	1 record audio	2	129
18	18	3 view Wi-Fi connections	2	8,60,61,13
19	19	5 view network connections	2	8,60,61,13
20	20	5 control flashlight	2	73
21	21	5 full network access	2	13,59
22	22	5 run at startup	2	125
23	23	5 control vibration	2	164
24	24	4 read the contents of your USB storage	3	110
25	25	4 modify or delete the contents of your USB storage	3	110,170
26	26	2 read the contents of your USB storage	3	110
27	27	2 modify or delete the contents of your USB storage	3	110,170
28	28	5 receive data from Internet	3	8,89
29	29	5 view network connections	3	8,60,61,13
30	30	5 full network access	3	13,59
31	31	5 run at startup	3	125
32	32	5 control vibration	3	164
33	33	5 prevent device from sleeping	3	165
34	34	7 approximate location (network-based)	4	2,3,4,5,64,84,91
35	35	2 modify or delete the contents of your USB storage	4	110,170
36	36	2 read the contents of your USB storage	4	110
37	37	4 modify or delete the contents of your USB storage	4	110,170
38	38	4 read the contents of your USB storage	4	110
39	39	5 pair with Bluetooth devices	4	42,43,44

Εικόνα 5. Ο πίνακας AppsPermissionsDetail της βάσης δεδομένων.

- ❖ **CATEGORIES:** Ο πίνακας αυτός περιέχει όλες τις κατηγορίες των εφαρμογών του Play Store με τα εξής πεδία:
 - Το Primary Key (**PK**),
 - Και το όνομα της κάθε κατηγορίας εφαρμογών του Play Store με όνομα πεδίου (**DESCR**).



Εικόνα 6. Ο πίνακας Categories της βάσης δεδομένων.

❖ **OSPERMISSIONS:** Ο πίνακας αυτός αποτελεί τον έναν από τους πιο σημαντικούς πίνακες μαζί με τον AppsPermissionsDetail, καθώς περιέχει όλες τις άδειες πρόσβασης του λειτουργικού συστήματος που θα μπορούσαν να ζητηθούν από το Android 6 και έπειτα. Τα πεδία του είναι τα εξής :

- Το Primary Key (**PK**),
- Και το όνομα οποιασδήποτε άδειας πρόσβασης του λειτουργικού Android (**DESCR**).

PK	DESCR
1	BATTERY_STATS
2	ACCESS_COARSE_LOCATION
3	ACCESS_FINE_LOCATION
4	ACCESS_LOCATION_EXTRA_COMMANDS
5	ACCESS_MOCK_LOCATION
6	ACCESS_NOTIFICATION_POLICY
7	ACCESS_SURFACE_FLINGER
8	ACCESS_WIFI_STATE
9	ACCOUNT_MANAGER
10	ADD_VOICEMAIL
11	ANSWER_PHONE_CALLS
12	AUTHENTICATE_ACCOUNTS
13	ACCESS_NETWORK_STATE
14	BIND_ACCESSIBILITY_SERVICE
15	BIND_APPWIDGET
16	ACCEPT_HANDOVER
17	ACCESS_CHECKIN_PROPERTIES
18	BIND_AUTOFILL_SERVICE
19	BIND_CARRIER_MESSAGING_SERVICE
20	BIND_CARRIER_SERVICES
21	BIND_CHOOSER_TARGET_SERVICE
22	BIND_CONDITION_PROVIDER_SERVICE
23	BIND_DEVICE_ADMIN
24	BIND_DREAM_SERVICE
25	BIND_INCALL_SERVICE
26	BIND_INPUT_METHOD
27	BIND_MIDI_DEVICE_SERVICE
28	BIND_NFC_SERVICE
29	BIND_NOTIFICATION_LISTENER_SERVICE
30	BIND_PRINT_SERVICE
31	BIND_QUICK_SETTINGS_TILE
32	BIND_REMOTEVIEWS
33	BIND_SCREENING_SERVICE
34	BIND_TELECOM_CONNECTION_SERVICE
35	BIND_TEXT_SERVICE
36	BIND_TV_INPUT
37	BIND_VISUAL_VOICEMAIL_SERVICE
38	BIND_VOICE_INTERACTION
39	BIND_VPN_SERVICE
40	BIND_VR_LISTENER_SERVICE
41	BIND_WALLPAPER
42	BLUETOOTH
43	BLUETOOTH_ADMIN
44	BLUETOOTH_PRIVILEGED
45	BODY_SENSORS
46	BRICK
47	BROADCAST_PACKAGE_REMOVED
48	BROADCAST_SMS

Εικόνα 7. Ο πίνακας OsPermissions της βάσης δεδομένων.

4.2.1 SQL Ερωτήματα

Τα δεδομένα των εφαρμογών του Google Play συλλέχτηκαν στη βάση δεδομένων, με σκοπό τη δημιουργία ερωτημάτων (queries) και στη συνέχεια, την εξαγωγή ορισμένων συμπερασμάτων που αφορούν τις εφαρμογές και τις άδειες πρόσβασης που αυτές ζητούν από τους χρήστες.

Τα SQL ερωτήματα που υλοποιήθηκαν για το σκοπό της παρούσας πτυχιακής εργασίας είναι τα εξής:

i. Πλήθος Αδειών Πρόσβασης ανά Εφαρμογή :

```
SELECT B.DESCR APP,COUNT(A.APPS) PERMISSIONS
FROM APPSPERMISSIONSDetail A
JOIN APPS B ON B.PK=A.APPS
GROUP BY B.DESCR
ORDER BY 2 DESC
```

ii. Πλήθος Αδειών Πρόσβασης ανά Κατηγορία :

```
SELECT C.DESCR, COUNT(D.APPS)
FROM APPS B
JOIN CATEGORIES C ON C.PK=B.CATEGORIES
JOIN APPSPERMISSIONSDetail D ON D.APPS=B.PK
GROUP BY C.DESCR
ORDER BY 2 DESC
```

iii. Οι 40 εφαρμογές που ζητούν τα περισσότερα δικαιώματα :

```
SELECT B.DESCR APP,COUNT(A.APPS) PERMISSIONS
FROM APPSPERMISSIONSDetail A
JOIN APPS B ON B.PK=A.APPS
GROUP BY B.DESCR
ORDER BY 2 DESC
LIMIT 40;
```

iv. Οι 30 εφαρμογές που ζητούν τα λιγότερα δικαιώματα :

```
SELECT A.APPS,B.DESCR,COUNT(A.APPSPERMISSIONS) plithos
FROM APPSPERMISSIONSDetail A
JOIN APPS B on B.PK=A.APPS
GROUP BY A.APPS,B.DESCR
ORDER by 3 ASC
LIMIT 30;
```

v. Οι 30 εφαρμογές που ζητούν τις περισσότερες επικίνδυνες άδειες:

```
SELECT* FROM
(SELECT DISTINCT C.DESCR,COUNT(A.CRUSIAL)
FROM APPSPERMISSIONS A
JOIN APPSPERMISSIONSDetail b on b.APPSPERMISSIONS=a.pk
JOIN APPS C on C.PK=B.APPS
WHERE A.CRUSIAL = 'true'
GROUP BY C.DESCR
) Z
ORDER BY 2 DESC;
LIMIT 30;
```

vi. Οι 30 άδειες που ζητούνται περισσότερο από τις εφαρμογές:

```
SELECT A.DESCR, count(A.DESCR)
FROM APPSPERMISSIONSDetail A
GROUP BY A.DESCR
ORDER BY 2 DESC;
```

vii. Οι 30 άδειες που ζητούνται λιγότερο από τις εφαρμογές:

```
SELECT A.DESCR, count(A.DESCR)
FROM APPSPERMISSIONSDetail A
GROUP BY A.DESCR
ORDER BY 2 ASC;
```

viii. Οι 30 άδειες που ζητούνται περισσότερο και το ποσοστό των εφαρμογών που τις ζητούν :

```
SELECT A.DESCR,COUNT(APPS),ROUND( CAST(COUNT(APPS)AS
REAL)/(SELECT COUNT(PK) FROM APPS) * 100 ,2)
PERCENTOFFERRMISSIONSINAPPS
FROM APPSPERMISSIONSDetail A
GROUP BY A.DESCR
ORDER BY 2 DESC;
```

ix. Οι επικίνδυνες άδειες και το ποσοστό εφαρμογών που τις ζητούν :

```
SELECT A.DESCR,COUNT(APPS),ROUND( CAST(COUNT(APPS)AS
REAL)/(SELECT COUNT(PK) FROM APPS) * 100 ,2)
PERCENTOFFERRMISSIONSINAPPS
,B.DESCR,B.CRUSIAL
FROM APPSPERMISSIONSDetail A
JOIN APPSPERMISSIONS B ON A.APPSPERMISSIONS=B.PK
WHERE B.CRUSIAL ='true'
GROUP BY A.DESCR
ORDER BY 2 DESC
```

4.2.2 Ανάλυση Κώδικα

```
using Newtonsoft.Json;
using System;
using System.Collections.Generic;
using System.Windows.Forms;

namespace ergasia
{
    public partial class Form1 : Form
    {
        SQLiteClass DB = null;
        List<System.Diagnostics.Process> ChromeDriver = null;
        GooglePlayClass google = null;
        public Form1()
        {
            InitializeComponent();
        }

        private void Form1_Load(object sender, EventArgs e)
        {
            try //Ελεγχος σφαλμάτων για να μη καταρρεύσει η εφαρμογή. Αν δεν τα καταφέρει πηγαίνει στο catch (88) και στην (112)
            αναφέρεται το σφάλμα.
            {
                //Αρχικοποίηση αντικειμένου βάσης.
                DB = new SQLiteClass(new SqliteLoginData { DBName = "Privacy_Policies.db" });
                //Ελεγχος σχήματος βάσης, Δημιουργία πινάκων βάσης.
                new SchemaClass(DB).CheckSchema();

                //Αρχικοποίηση αντικειμένου google(είναι συλλογή που περιέχει μεθόδους που αφορούν το GooglePlay
                GetCategories,GetAppsByCategories κ.τ.λ. )
                google = new GooglePlayClass(DB);
                //Αρχικοποίηση του ChromeDriver, μιας τρίτης βιβλιοθήκης που εξομοιώνει την πλοήγηση σε site με κώδικα
                ChromeDriver = google.GetChromeDriver();

                //Διάβασμα και ανάθεση κατηγοριών στην lc που είναι τύπου List<AppCategories>
                List<AppCategories> lc = google.GetCategories();
                //Αρχικοποίηση λίστας αλφαριθμητικών cat
                List<string> cat = new List<string>();
            }
        }
    }
}
```

```

//Αρχικοποίηση και εκκίνηση διαδικασίας εισαγωγής δεδομένων στην βάση
DB.ExcuteSql("begin");
//Για κάθε apc τύπου AppCategories που είναι στην λίστα lc
foreach (AppCategories apc in lc)
{
    //Εισαγωγή περιγραφής κατηγορίας στην βάση
    DB.ExcuteSql("INSERT INTO CATEGORIES (DESCR) VALUES (@p1)", new object[] { apc.DESCR.Replace("&",
"_AND_").Replace(" ", "") });
    //Φόρτωση λίστας κατηγοριών στην λίστα από αλφαριθμητικά cat
    cat.Add(apc.DESCR.Replace("&", "_AND_").Replace(" ", ""));
}
//Τέλος εισαγωγής εγγραφών στον πίνακα CATEGORIES και οριστικοποίηση (commit)
DB.ExcuteSql("end");
//Δημιουργία λίστας αλφαριθμητικών από την λίστα cat
string[] DoCategories = cat.ToArray();

//Βρόγχος για κάθε στοιχείο της DoCategories
for (int i = 0; i < DoCategories.Length; i++)
{
    //Αρχικοποίηση και ανάθεση της List<Apps> apps(λίστα από εφαρμογές) από την μέθοδο GetAppsByCategories με
    παράμετρο την ονομασία της κατηγορίας
    List<Apps> apps = google.GetAppsByCategories(DoCategories[i]);
    //Αν η κατηγορία είναι άδεια, go next
    if (apps == null) continue;
    //Για κάθε εφαρμογή apc στην λίστα apps
    foreach (Apps apc in apps)
    {
        //Αρχικοποίηση εισαγωγής δεδομένων στην βάση.
        DB.ExcuteSql("begin");
        try //Έλεγχος σφαλμάτων για να μη καταρρεύσει η εφαρμογή. Αν δεν τα καταφέρει πηγαίνει στο catch (106).

        //Εισαγωγή δεδομένων στοιχείων της εφαρμογής. Τα δεδομένα στη βάση περνιούνται με παραμέτρους για την
        ασφάλεια της βάσης δεδομένων.
        apc.PK = DB.ExcuteSqlInt("INSERT INTO APPS (DESCR,COMPANY,CATDESCR,CATEGORIES,URLREF) VALUES
(@p1,@p2,@p3,@p4,@p5)",
            new object[] { apc.DESCR, apc.COMPANY, apc.CATEGORY, apc.CATEGORIES, apc.URLREF }, "APPS");
    }
}

```


4.3 Μελέτη των Πολιτικών Ιδιωτικότητας Δέκα Δημοφιλών Εφαρμογών Android ως προς τα Δεδομένα που Συλλέγουν

Σε αυτήν την ενότητα θα εξετάσουμε τις πολιτικές ιδιωτικότητας των δέκα πιο δημοφιλών εφαρμογών στο Play Store της Google. Θα μελετηθούν τα προσωπικά δεδομένα που αυτές συλλέγουν από τους χρήστες καθώς το σκοπό και τη χρήση των δεδομένων αυτών.

Η αναγνωσιμότητα των εφαρμογών από τους χρήστες αποτέλεσε την πιο σημαντική παράμετρο για την επιλογή των εφαρμογών καθώς όλες διαθέτουν δισεκατομμύρια λήψεις στο Google Play. Παράλληλα, σημαντικό ρόλο για την επιλογή των εφαρμογών αποτέλεσε η χρήση επικίνδυνων δικαιωμάτων των χρηστών όπως κάμερα, μικρόφωνο, αποθηκευτικός χώρος, κατάσταση τηλεφώνου. Επίσης, οι εφαρμογές επιλέχτηκαν βάση της σχετικότητας των λειτουργιών τους ανά δυο, λ.χ. Netflix-Stremio, Zoom-Skype, έτσι ώστε να μπορούν να συγκριθούν οι πολιτικές ιδιωτικότητας τους, εν συνεχεία.

1. Facebook

Το Facebook αποτελεί το μεγαλύτερο και πιο διαδεδομένο κοινωνικό δίκτυο αλλά και ένας ιστότοπος με χρήστες περισσότερους από 2.50 εκατομμύρια μέχρι το 2019. Μέσω του Facebook οι χρήστες ανταλλάζουν απόψεις, τραγούδια, οπτικοακουστικό υλικό αλλά και πληροφορίες τοποθεσίας, δεδομένα τα οποία κρίνονται ευαίσθητα, και γι' αυτό η μελέτη του κρίνεται απαραίτητη. [\[20\]](#)

ΤΙ ΕΙΔΟΥΣ ΠΛΗΡΟΦΟΡΙΕΣ ΣΥΛΛΕΓΕΙ

Το Facebook χωρίζει τις πληροφορίες που συλλέγει σε τρεις επιμέρους κατηγορίες :

- **Πληροφορίες οι οποίες προέρχονται από ενέργειες τις οποίες ο χρήστης κοινοποιεί**
 - Συλλογή περιεχομένου από επικοινωνία, ανταλλαγή μηνυμάτων, κοινοποίηση υλικού, δημιουργία λογαριασμού . Τα περιεχόμενα αυτά μπορεί να περιέχουν μεταδεδομένα όπως για παράδειγμα την τοποθεσία στην οποία τραβήχτηκε μια φωτογραφία, πληροφορίες σχετικές με την κάμερα κ.α.
 - Συλλογή πληροφοριών για τις ομάδες, τις σελίδες, τους λογαριασμούς, τα hashtags, και τα άτομα με τα οποία έχει επαφή ο χρήστης.
 - Στοιχεία επικοινωνίας, όταν ο χρήστης επιθυμεί να τα γνωστοποιήσει, όπως κατάλογο επαφών, ιστορικό κλήσεων ή SMS.

- Συλλογή του περιεχομένου που παρακολουθεί ο χρήστης, λειτουργίες και ενέργειες του χρήστη καθώς και τις ώρες, τη συχνότητα και διάρκεια των ενεργειών αυτών.
- Συγκέντρωση στοιχείων που αφορούν τις αγορές του χρήστη μέσω της εφαρμογής, όπως για παράδειγμα στοιχεία της κάρτας, στοιχεία επαλήθευσης λογαριασμού, πληροφορίες τιμολόγησης, διεύθυνση αποστολής καθώς και στοιχεία επικοινωνίας.
- Λήψη πληροφοριών από τρίτα άτομα που χρησιμοποιούν την εφαρμογή και σχετίζονται με τον εκάστοτε χρήστη. Για παράδειγμα κοινοποίηση ή σχολιασμός μιας φωτογραφίας του χρήστη, αποστολή μηνύματος ή εισαγωγή των στοιχείων επικοινωνίας.

➤ **Πληροφορίες Συσκευής**

- Συλλογή πληροφοριών σχετικά με τους υπολογιστές, τα κινητά, τις τηλεοράσεις και γενικότερα όλες τις συνδεδεμένες συσκευές που χρησιμοποιεί και συνδέεται ο χρήστης.
- Από τις συσκευές αυτές η εφαρμογή λαμβάνει πληροφορίες όπως το λειτουργικό σύστημα, την έκδοση υλικού και λογισμικού, τα επίπεδα μπαταρίας, την ισχύ του σήματος, το διαθέσιμο χώρο αποθήκευσης, τον τύπο προγράμματος περιήγησης, τα ονόματα και τους τύπους εφαρμογών και τέλος τα πρόσθετα (Plugins) .
- Πληροφορίες για τις λειτουργίες και τις συμπεριφορές που ακολουθούνται στη συσκευή όπως για παράδειγμα πληροφορίες για τη χρήση του ποντικιού, έτσι ώστε η εφαρμογή να μπορεί να διακρίνει μεταξύ χρηστών και bots.
- Συλλογή μοναδικών αναγνωριστικών και αναγνωριστικά συσκευών, όπως για παράδειγμα παιχνίδια, εφαρμογές ή λογαριασμούς που χρησιμοποιεί ο χρήστης, αλλά και αναγνωριστικά οικογενειακών συσκευών.
- Πληροφορίες που αφορούν σήματα Bluetooth και κοντινά σημεία πρόσβασης σε δίκτυα WIFI, αναμεταδότες και πύργους κινητής τηλεφωνίας.
- Δεδομένα τα οποία ο χρήστης επιτρέπει την πρόσβαση της εφαρμογής σε αυτά, όπως δεδομένα GPS, κάμερας και φωτογραφιών.
- Συλλογή πληροφοριών όπως το όνομα του παρόχου κινητής τηλεφωνίας ή υπηρεσιών δικτύου, τη γλώσσα, τη ζώνη ώρας, τον αριθμό του κινητού τηλεφώνου, τη διεύθυνση IP, τη ταχύτητα σύνδεσης αλλά και πληροφορίες για άλλες συσκευές που βρίσκονται κοντά ή στο δίκτυο του χρήστη.
- Πληροφορίες που συλλέγονται από τα Cookies.

➤ **Πληροφορίες από Συνεργάτες**

- Οι διαφημιζόμενοι, οι προγραμματιστές εφαρμογών και οι εκδότες μπορούν να αποστέλλουν πληροφορίες στην εφαρμογή για το χρήστη μέσω των plugins, των API, των SDK και του Pixel του Facebook. Οι συνεργάτες αυτοί μπορούν να παρέχουν πληροφορίες για τις δραστηριότητες του χρήστη εκτός Facebook, όπως πληροφορίες για τη συσκευή του χρήστη, τις ιστοσελίδες που επισκέπτεται, τις αγορές και τις διαφημίσεις που παρακολουθεί, κάνοντας χρήση του API του, χωρίς καν να χρειαστεί να έχει λογαριασμό στην εφαρμογή Facebook.

ΤΡΟΠΟΣ ΧΡΗΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Το Facebook χρησιμοποιεί τα δεδομένα που συλλέγει για τους παρακάτω σκοπούς:

- Παροχή, εξατομίκευση και βελτίωση των προϊόντων της.
- Παροχή μετρήσεων, στατιστικών στοιχείων και άλλων επαγγελματικών υπηρεσιών.
- Προώθηση προστασίας, ακεραιότητας και ασφάλειας.
- Επικοινωνία με τους χρήστες για την ενημέρωσή τους όσον αφορά τις πολιτικές και τους όρους της εφαρμογής.
- Έρευνα και καινοτομία προς όφελος του κοινωνικού συνόλου, σε τομείς όπως τεχνολογική εξέλιξη, δημόσιο συμφέρον, υγεία και ευημερία.

ΚΟΙΝΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΕΣ ΟΝΤΟΤΗΤΕΣ

Το Facebook κοινοποιεί τα προσωπικά δεδομένα των χρηστών του, με στόχο τη βελτίωση των προϊόντων του, σε συνεργάτες όπως :

- **Συνεργάτες που χρησιμοποιούν τις υπηρεσίες αναλύσεων του Facebook και σε συνεργάτες μετρήσεων.**

Η εφαρμογή παρέχει στοιχεία και πληροφορίες που βοηθούν τις τρίτες οντότητες να κατανοήσουν πως ο χρήστης αλληλοεπιδρά με τις δημοσιεύσεις, τις καταχωρήσεις, τις σελίδες και το περιεχόμενο του Facebook.

- **Διαφημιζόμενοι.**

Στους διαφημιζόμενους του, το Facebook παρέχει δημογραφικά στοιχεία όπως για παράδειγμα ηλικία και περιοχή, των ανθρώπων που ενδιαφέρονται για την εκάστοτε διαφήμιση, έτσι ώστε να κατανοήσουν καλύτερα το κοινό τους. Παράλληλα, η εφαρμογή δεν

κοινοποιεί πληροφορίες ταυτοποίησης χρήστη όπως email, ή τηλέφωνο, εκτός εάν ο χρήστης δώσει την συγκατάθεση του.

➤ ***Συνεργάτες που προσφέρουν αγαθά και υπηρεσίες στα προϊόντα του Facebook.***

Στην περίπτωση που ο χρήστης αγοράσει κάποιο αγαθό μέσω ενός πωλητή του Facebook, αυτομάτως μπορεί να έχει πρόσβαση στις δημόσιες πληροφορίες του χρήστη καθώς και στα στοιχεία της αγοράς, όπως λεπτομέρειες αποστολής και στοιχεία επικοινωνίας.

➤ ***Προμηθευτές και Πάροχοι Υπηρεσιών.***

Παροχή πληροφοριών και περιεχομένου σε προμηθευτές και παρόχους υπηρεσιών που υποστηρίζουν το Facebook σε επιχειρησιακό επίπεδο.

➤ ***Ερευνητές και Ακαδημαϊκοί.***

Παροχή δεδομένων σε ερευνητές και ακαδημαϊκούς με σκοπό τη διεξαγωγή ερευνών.

➤ ***Επιβολή Νόμου ή Νομικά Αιτήματα.***

Κοινοποιούνται πληροφορίες στις διωκτικές αρχές για νομικά ζητήματα.

(Ημερομηνία τελευταίας αναθεώρησης πολιτικής ιδιωτικότητας Facebook: 21 Αυγούστου 2020)

2. Twitter

Το Twitter αποτελεί επίσης έναν πολύ διαδεδομένο ιστοχώρο κοινωνικής δικτύωσης όπου επιτρέπει στους χρήστες του να στέλνουν και να διαβάζουν σύντομα μηνύματα, μέχρι 280 χαρακτήρες, τα οποία ονομάζονται “τουίτς” (tweets). Η εφαρμογή δημιουργήθηκε το 2006, απέκτησε γρήγορα αναγνώριση και σήμερα αγγίζει τους 400 εκατομμύρια χρήστες το μήνα.^[21] Ως κοινωνικό δίκτυο το οποίο διαχειρίζεται τα προσωπικά δεδομένα των χρηστών, κρίθηκε απαραίτητη η μελέτη της πολιτικής ιδιωτικότητας του.

Μελετώντας την πολιτική ιδιωτικότητας του Twitter, παρατηρήθηκε πως οι πληροφορίες διαχωρίζονται σε αυτές που ο χρήστης διαμοιράζεται με το Twitter, και στις πληροφορίες που παίρνονται αυτοματοποιημένα από την εφαρμογή . ^[22]

➤ **Πληροφορίες που Διαμοιράζει ο Χρήστης**

- Στην περίπτωση όπου ο χρήστης δημιουργήσει λογαριασμό, παραχωρεί στην εφαρμογή βασικά προσωπικά του δεδομένα, όπως όνομα, κωδικό, email και κινητό τηλέφωνο.
- Οι περισσότερες πληροφορίες στο Twitter είναι δημόσιες, όπως για παράδειγμα πληροφορίες στο προφίλ του χρήστη, ώρα και ημερομηνία ανάρτησης των tweets, τοποθεσία και όλες οι αλληλεπιδράσεις με τρίτες οντότητες. Παράλληλα, για τη δημοσιοποίηση των tweet των χρηστών σε άλλες ιστοσελίδες, το Twitter χρησιμοποιεί το API του. [\[23\]](#)
- Συλλογή στοιχείων επικοινωνίας του χρήστη όπως κινητό και διεύθυνση ταχυδρομείου, με σκοπό την αυθεντικοποίηση του.
- Το Twitter παρέχει τη λειτουργία των προσωπικών μηνυμάτων και αποθηκεύει τους χρήστες με τους οποίους έχει επικοινωνήσει ένας λογαριασμός, χωρίς την αποθήκευση του περιεχομένου της συνομιλίας. Παράλληλα, σαρώνει τα προσωπικά μηνύματα για ιούς, κακόβουλο λογισμικό, απαγορευμένους συνδέσμους και εικόνες.
- Συλλογή στοιχείων που αφορούν ηλεκτρονικές αγορές όπως για παράδειγμα πληροφορίες χρεωστικής ή πιστωτικής κάρτας, ημερομηνία λήξης της κάρτας, CVV, κ.α.

➤ **Πληροφορίες που καταχωρεί αυτοματοποιημένα το Twitter**

- Δεδομένα τοποθεσίας τα οποία παίρνονται μέσω της διεύθυνσης IP ή των ρυθμίσεων της συσκευής για την παροχή υπηρεσιών στο χρήστη.
- Διευθύνσεις τις οποίες επισκέπτεται ο χρήστης είτε από διαφημιστικά email του Twitter είτε από "Tweets".
- Συλλογή των cookies για την συγκέντρωση πρόσθετων πληροφοριών καθώς και για την καλύτερη λειτουργία των υπηρεσιών του Twitter.
- Συλλογή δεδομένων του χρήστη για την προβολή διαφημίσεων σχετικών με τα ενδιαφέροντα του. Συνεπώς, το Twitter λαμβάνει πληροφορίες για το περιεχόμενο το οποίο ο χρήστης παρακολουθεί, καθώς και οποιαδήποτε αλληλεπίδραση με τις υπηρεσίες του. Αυτά τα δεδομένα καταγραφής ή αλλιώς "Log Data", περιλαμβάνουν πληροφορίες όπως η διεύθυνση IP, ο τύπος προγράμματος περιήγησης, το λειτουργικό σύστημα, πληροφορίες συσκευής και cookies, καθώς και την εταιρεία κινητής τηλεφωνίας.
- Εφόσον ο χρήστης προβάλλει περιεχόμενο του Twitter, σε τρίτες οντότητες που ενσωματώνουν περιεχόμενο του, τότε το Twitter λαμβάνει δεδομένα καταγραφής για την ιστοσελίδα την οποία επισκέφθηκε. Αυτές οι πληροφορίες συλλέγονται

για την καλύτερη κατανόηση των υπηρεσιών της εφαρμογής, την προστασία και την ασφάλεια της πλατφόρμας καθώς και την εμφάνιση σχετικών διαφημίσεων ανάλογα με τα ενδιαφέροντα του εκάστοτε χρήστη.

➤ ***Κοινοποίηση Δεδομένων σε Τρίτες Οντότητες***

- Σε παροχές υπηρεσιών.
- Σε διαφημιστές.
- Σε περίπτωση αλλαγής της ιδιοκτησίας του Twitter.
- Σε περίπτωση που απαιτηθούν από την κυβέρνηση ή τον νόμο.

*(Ημερομηνία τελευταίας αναθεώρησης πολιτικής ιδιωτικότητας
Twitter: 18 Ιουνίου 2020)*

3.Viber

Το Viber αποτελεί ακόμη μια πολύ επιτυχημένη εφαρμογή η οποία βασίζεται στην ανταλλαγή άμεσων μηνυμάτων. Η εφαρμογή προορίζεται για smartphones, tablets πλέον και για υπολογιστές και αναπτύχθηκε από την εταιρεία Viber Media. Οι χρήστες εκτός από μηνύματα, μπορούν να ανταλλάσσουν φωτογραφίες, βίντεο καθώς και μηνύματα πολυμέσων ήχου. Το λογισμικό είναι διαθέσιμο σε λειτουργικά Apple, Android, Blackberry, Nokia Series 40, Symbian, Bada, Windows Phone και Microsoft Windows. Το Viber ξεκίνησε τη λειτουργία του στις συσκευές iPhone το 2010 και η απήχηση στο κοινό ήταν πολύ μεγάλη. Σήμερα καταγράφονται 260 εκατομμύρια χρήστες Viber μηνιαίως, αριθμός αρκετά ικανοποιητικός για να προβούμε σε μελέτη της πολιτικής ιδιωτικότητας του. [\[24\]](#)

➤ ***Πληροφορίες που Συλλέγει το Viber***

- Το Viber επιβεβαιώνει τους χρήστες του πως οι προσωπικές τους πληροφορίες αποθηκεύονται και συλλέγονται, παρόλα αυτά δεν διαβάζονται από τους διαχειριστές των δεδομένων. Επιπλέον, τα δεδομένα αυτά διαγράφονται από τους servers της εφαρμογής εάν ο χρήστης απενεργοποιήσει το λογαριασμό του.
- Συλλογή πληροφοριών λογαριασμού όπως όνομα, διεύθυνση λογαριασμού, ημερομηνία γέννησης, ηλικία, τηλέφωνο καθώς και πληροφορίες συναλλαγών όπου χρειάζεται. Επιπλέον, η εφαρμογή αποκτά πρόσβαση στις επαφές του χρήστη, δημιουργώντας αντίγραφο στα αρχεία της εάν αυτό εγκριθεί από το χρήστη.
- Αν ο χρήστης συνδεθεί στο Viber του, μέσω Facebook, Twitter, VK και γενικότερα μέσω τρίτης οντότητας, ο χρήστης

αυτόματα παρέχει άδεια συλλογής πληροφοριών στην εφαρμογή. Οι πληροφορίες μπορεί να είναι το προφίλ, οι φίλοι, λογαριασμοί που ακολουθεί ο χρήστης ή τον ακολουθούν, διεύθυνση ταχυδρομείου, ημερομηνία γέννησης, πληροφορίες εργασίας και εκπαίδευσης, ενδιαφέροντα καθώς και τοποθεσία .

- ο Συλλογή πληροφοριών δραστηριότητας και κατάστασης. Οι υπόλοιποι χρήστες γνωρίζουν την κατάσταση σύνδεσης του χρήστη, αν διαβάστηκε κάποιο μήνυμα ή όχι, αν βρίσκεται σε κλήση και τη διάρκεια αυτής. Αυτές οι πληροφορίες μπορούν να γίνουν άορατες εάν ο χρήστης προβεί σε επεξεργασία των ρυθμίσεων.
- ο Καταχώρηση δεδομένων όσον αφορά τις ιστοσελίδες που επισκέπτεται ο χρήστης, τα Like και τα σχόλια. Επίσης, συλλέγονται πληροφορίες για τα παιχνίδια που προτιμά και τα προϊόντα που επιθυμεί να αγοράσει.
- ο Πληροφορίες για τη συσκευή από την οποία συνδέθηκε ο χρήστης στο Viber, όπως το μοναδικό αναγνωριστικό της συσκευής, το λειτουργικό της σύστημα, τον περιηγητή αναζήτησης, το ασύρματο δίκτυο, τον πάροχο κινητής τηλεφωνίας καθώς και την τοποθεσία του χρήστη σε περίπτωση που αυτός το εγκρίνει.

➤ **Τρόπος Χρήσης των Δεδομένων**

- ο Για τη δημιουργία λογαριασμού, προφίλ και του Viber ID.
- ο Για το συγχρονισμό μεταξύ συσκευών.
- ο Για την εξατομίκευση της εμπειρίας του χρήστη παρέχοντας περιεχόμενο όπως διαφημίσεις ή παιχνίδια, σχετικά με αυτόν.
- ο Για ενέργειες πληρωμών του χρήστη.
- ο Για την επίτευξη της επικοινωνίας με τους άλλους χρήστες, την προβολή των επαφών του που διαθέτουν ήδη Viber και την ενημέρωση του για εγγραφή νέων μελών από τη λίστα επαφών του.
- ο Για τη βελτίωση των υπηρεσιών του.
- ο Για την αποτροπή, τον εντοπισμό και τη διερεύνηση απατών, παραβιάσεων ασφάλειας, παράνομων δραστηριοτήτων και στην πραγματικότητα για την επιβολή των όρων χρήσης.
- ο Σε περίπτωση που ζητηθούν από το νόμο.
- ο Σε περίπτωση επικοινωνίας όπου ο χρήστης αντιμετωπίζει κάποιο πρόβλημα.

(Ημερομηνία τελευταίας αναθεώρησης πολιτικής ιδιωτικότητας Viber: Νοέμβριος 2019)

4. WhatsApp

Το WhatsApp αποτελεί μια επίσης πολύ διαδεδομένη εφαρμογή ανταλλαγής μηνυμάτων όπως το Viber. Οι χρήστες μπορούν να στείλουν εικόνες, βίντεο, ήχους και μηνύματα πολυμέσων. Το λογισμικό είναι διαθέσιμο για λειτουργικά Apple, Android, Blackberry, Nokia Series 40, Symbian και Windows Phone. Η εφαρμογή ιδρύθηκε το 2009 από τους δημιουργούς του Yahoo! και η απήχηση είναι εξίσου τεράστια καθώς καταγράφει 68 εκατομμύρια χρήστες μόνο στην Αμερική το 2019.

Στην πολιτική ιδιωτικότητας του WhatsApp, όπως και σε αυτή του Facebook, οι πληροφορίες που συλλέγονται από την εφαρμογή, χωρίζονται σε τρεις επιμέρους κατηγορίες. [\[25\]](#)

➤ Πληροφορίες που Παρέχει ο Χρήστης

- ο Πληροφορίες για τη δημιουργία λογαριασμού του χρήστη όπως κινητό τηλέφωνο, όνομα, φωτογραφία προφίλ, καθώς και όλες τις επαφές του, ανεξαρτήτως από το αν διαθέτουν λογαριασμό WhatsApp.
- ο Περιεχόμενο μηνυμάτων με βίντεο, εικόνα ή και ήχο διαγράφονται αυτόματα από τους servers της εφαρμογής μόλις σταλούν επιτυχώς στον παραλήπτη. Αν ένα μήνυμα δεν σταλθεί απευθείας, αποθηκεύεται κρυπτογραφημένο στους servers της εφαρμογής για 30 μέρες, και στη συνέχεια διαγράφεται.
- ο Πληροφορίες επικοινωνίας οι οποίες θα χρησιμοποιηθούν για πιθανή εξυπηρέτηση του πελάτη, από την εφαρμογή.

➤ Πληροφορίες οι οποίες παίρνονται αυτοματοποιημένα από την εφαρμογή

- ο Συλλογή πληροφοριών που αφορούν τη δραστηριότητα του χρήστη στις υπηρεσίες της εφαρμογής όπως ποιες υπηρεσίες προτιμά, ποια η αλληλεπίδραση με τους άλλους χρήστες.
- ο Πληροφορίες που αφορούν πληρωμές μέσω του WhatsApp ή τρίτων οντοτήτων.
- ο Πληροφορίες συσκευής όπως το λειτουργικό σύστημα, την έκδοση της εφαρμογής, την διεύθυνση IP, το πρόγραμμα περιήγησης, το ποσοστό μπαταρίας και το δίκτυο κινητής τηλεφωνίας.
- ο Χρήση Cookies για τη βελτίωση της εμπειρίας του χρήστη.
- ο Συλλογή πληροφοριών για την κατάσταση σύνδεσης του χρήστη, δηλαδή αν είναι ενεργός ή πόσες μέρες έχει να χρησιμοποιήσει την εφαρμογή.

➤ **Κοινοποίηση Δεδομένων σε Τρίτες Οντότητες**

- Πληροφορίες που παρέχουν άλλοι χρήστες που αλληλοεπιδρούν με τον χρήστη όπως αριθμό κινητού τηλεφώνου, όνομα κ.α.
- Πληροφορίες από επιχειρήσεις με τις οποίες συνεργάζεται το WhatsApp, οι οποίες βοηθούν στη λειτουργία, την παροχή, τη βελτίωση, την κατανόηση και την υποστήριξη των διαθέσιμων υπηρεσιών στους χρήστες. Τέτοιες επιχειρήσεις θα μπορούσαν να βοηθούν με τη διεκπεραίωση πληρωμών, την παροχή πληροφοριών και χαρτών, την παροχή υποδομών κ.α.
- Πληροφορίες από παροχείς τρίτης οντότητας με τους οποίους συνεργάζεται το WhatsApp εφόσον ο χρήστης χρησιμοποιήσει την εφαρμογή μέσω των τρίτων οντοτήτων.

➤ **Τρόπος Χρήσης των Δεδομένων**

- Βελτίωση, διόρθωση και προσαρμογή των υπηρεσιών που προσφέρει το WhatsApp στους χρήστες του.
- Χρήση των στοιχείων του χρήστη έτσι ώστε να απαντήσουν οι τεχνικοί της εφαρμογής όταν ο χρήστης θέλει να επικοινωνήσει μαζί τους για τυχόν προβλήματα ή ερωτήσεις.
- Για την ασφάλεια και την προστασία του χρήστη.
- Επικοινωνία μεταξύ εφαρμογής και χρήστη για την ενημέρωση του ως προς τις υπηρεσίες και τις λειτουργίες που προσφέρει η εφαρμογή.
- Επικοινωνία μεταξύ του χρήστη και τρίτων οντοτήτων μέσω του WhatsApp, για παράδειγμα για την διεκπεραίωση μιας συναλλαγής, για την ενημέρωση περί προϊόντων και διαφημίσεων κ.α.
- Μετρήσεις και αναλύσεις.

(Ημερομηνία τελευταίας αναθεώρησης πολιτικής ιδιωτικότητας WhatsApp: 2020)

5. Netflix

Το Netflix αποτελεί μια συνδρομητική τηλεόραση όπου χρήστες έναντι μιας μηνιαίας συνδρομής, ενοικιάζουν ταινίες και σειρές. Το εύρος αυτών είναι τεράστιο, και από το 2013 το Netflix έχει προβεί σε δική του βιομηχανία παραγωγής ταινιών και σειρών με μεγάλη επιτυχία. Η εφαρμογή δημιουργήθηκε τον Απρίλιο του 1998 κάνοντας την επανάσταση στον τρόπο με τον οποίο το κοινό καταναλώνει το τηλεοπτικό και κινηματογραφικό προϊόν.[\[26\]](#) Με 167 εκατομμύρια χρήστες το 2019, είναι επιτακτική η ανάγκη μελέτης της πολιτικής ιδιωτικότητας του Netflix, έτσι ώστε να

προσδιορισθεί ο τρόπος με τον οποίο διαχειρίζεται τα δεδομένα εκατομμύρια χρηστών. [\[27\]](#)

Όπως και σε προηγούμενες εφαρμογές έτσι και στην παρούσα, οι πληροφορίες που αντλούνται κατηγοριοποιούνται στις επιμέρους:

➤ **Πληροφορίες που παρέχει ο χρήστης**

- Προσωπικές πληροφορίες κατά τη δημιουργία λογαριασμού όπως όνομα, κινητό τηλέφωνο, διεύθυνση ταχυδρομείου, ταχυδρομικό κώδικα και στοιχεία πληρωμών. Τα δεδομένα αυτά αντλούνται και σε περίπτωση επικοινωνίας του χρήστη με την εξυπηρέτηση πελατών, συμμετοχής σε έρευνες ή προωθητικές ενέργειες μάρκετινγκ.
- Πληροφορίες που παρέχει ο χρήστης κατά την υποβολή βαθμολογιών σε ταινίες, όπως προσωπικές προτιμήσεις ή ρυθμίσεις λογαριασμού.

➤ **Πληροφορίες οι οποίες παίρνονται αυτοματοποιημένα από την εφαρμογή**

- Συλλογή δεδομένων που αφορούν την αλληλεπίδραση του χρήστη με τις υπηρεσίες της εφαρμογής και τις διαφημίσεις.
- Καταχώρηση πληροφοριών σχετικά με τις επιλογές ταινιών, εκπομπών που έχει παρακολουθήσει ο χρήστης και ιστορικό αναζήτησης.
- Πληροφορίες από τις αλληλεπιδράσεις των χρηστών με τα email, τις ειδοποιήσεις και τα μηνύματα κειμένου που στέλνει το Netflix .
- Λεπτομέρειες που αφορούν την επικοινωνία του χρήστη με την εξυπηρέτηση πελατών της εφαρμογής, όπως ημερομηνία, ώρα και λόγο επικοινωνίας, αντίγραφα συνομιλιών και κινητό τηλέφωνο.
- Αναγνωριστικά συσκευών συμπεριλαμβανομένων και αυτών που υποστηρίζουν Netflix και βρίσκονται στο δίκτυο Wi-Fi του χρήστη.
- Καταχώρηση χαρακτηριστικών συσκευών και λογισμικού, όπως στοιχεία σύνδεσης, διεύθυνση IP άρα και τοποθεσία, πρόγραμμα περιήγησης και πληροφορίες σχετικά με το αρχείο καταγραφής διακομιστή παγκοσμίου ιστού.
- Πληροφορίες οι οποίες συλλέγονται μέσω Cookies.

➤ **Πληροφορίες που συλλέγονται από Συνεργάτες**

Συνεργάτες του χρήστη θεωρούνται οποιεσδήποτε εταιρείες έχουν αλληλεπίδραση με το χρήστη όπως ο πάροχος υπηρεσιών

τηλεόρασης ή διαδικτύου, πάροχοι συσκευών με δυνατότητα streaming μέσω των οποίων είναι διαθέσιμη η υπηρεσία του Netflix κ.α. Οι πληροφορίες που μοιράζονται οι συνεργάτες με την εφαρμογή ποικίλουν ανάλογα με τη μορφή των υπηρεσιών του συνεργάτη και δύνανται να περιλαμβάνουν:

- Ερωτήματα αναζήτησης τα οποία υποβάλλει ο χρήστης μέσω συσκευών ή ψηφιακών βοηθών και αφορούν το Netflix.
- Πληροφορίες ενεργοποίησης υπηρεσιών όπως της διεύθυνσης ηλεκτρονικού ταχυδρομείου ή άλλων στοιχείων επικοινωνίας.
- Διευθύνσεις IP, αναγνωριστικά συσκευών που υποστηρίζουν τον έλεγχο ταυτότητας χρήστη, την εμπειρία εγγραφής στο Netflix και τη διαδικασία διεκπεραίωσης πληρωμών του συνεργάτη.

➤ **Πληροφορίες από άλλες Πηγές**

Ορισμένες φορές το Netflix λαμβάνει πληροφορίες και από άλλες πηγές. Αυτές, διαφέρουν κατά καιρούς όμως μπορεί να περιλαμβάνουν:

- Παρόχους υπηρεσιών που βοηθούν στον εντοπισμό μιας τοποθεσίας με βάση της διεύθυνση IP ενός χρήστη.
- Παρόχους υπηρεσιών πληρωμής, οι οποίοι παρέχουν στοιχεία πληρωμής.
- Παρόχους δεδομένων οι οποίοι προμηθεύουν στο Netflix δημογραφικά ή δεδομένα που αφορούν τα ενδιαφέροντα των χρηστών ή τις διαφημίσεις.
- Διαθέσιμες πληροφορίες από δημόσιες αναρτήσεις σε μέσα κοινωνικής δικτύωσης.

➤ **Τρόπος Χρήσης των Δεδομένων**

- Για την παροχή, ανάλυση, διαχείριση, βελτίωση και εξατομίκευση των υπηρεσιών και των ενεργειών μάρκετινγκ.
- Για την επεξεργασία της εγγραφής, των παραγγελιών και των πληρωμών.
- Για τον προσδιορισμό της γεωγραφικής τοποθεσίας του χρήστη και την επίλυση τυχόν προβλημάτων δικτύου.
- Για την αποτροπή και τον εντοπισμό παράνομων δραστηριοτήτων.
- Για την ανάλυση και κατανόηση του κοινού της εφαρμογής, τη βελτίωση και βελτιστοποίηση του αλγορίθμου προτάσεων ταινιών.
- Για την επικοινωνία της εφαρμογής με το χρήστη για νέες κυκλοφορίες, λειτουργίες και περιεχόμενο.

➤ **Γνωστοποίηση των Πληροφοριών σε Τρίτες Οντότητες**

- Στον όμιλο εταιρειών του Netflix.
- Στους παρόχους υπηρεσιών οι οποίοι μπορεί να είναι πάροχοι υπηρεσιών μάρκετινγκ, διαφήμισης, διεκπεραιωτές συναλλαγών και πληρωμών κ.α.
- Στους συνεργάτες, προκειμένου να υπάρξει συντονισμός ως προς την παροχή της υπηρεσίας Netflix στα μέλη.
- Σε προωθητικές προσφορές, όπου οι εν λόγω τρίτες οντότητες είναι υπεύθυνες για τις δικές τους πρακτικές προστασίας απορρήτου.
- Στην Δημόσια Αρχή σε περίπτωση ανάγκης προστασίας της εφαρμογής σε τυχόν παραβιάσεις ή παράνομες πράξεις.
- Σε περίπτωση μεταβίβασης της εταιρείας σε τρίτους.

(Ημερομηνία τελευταίας αναθεώρησης πολιτικής ιδιωτικότητας Netflix: 31 Ιουλίου 2020)

6. Stremio

Το Stremio αποτελεί ένα media center ανοικτού κώδικα μέσω του οποίου μπορεί ο χρήστης να αναζητήσει και να παρακολουθήσει ταινίες, σειρές αλλά και κανάλια τηλεόρασης από δεκάδες χώρες, μεταξύ των οποίων και η Ελλάδα.

Ο τρόπος λειτουργίας του είναι διαφορετικός από αυτόν του Netflix. Το περιεχόμενο του αντλείται από πολλές πηγές, οι οποίες αποτελούνται κυρίως από torrents, γεγονός που το κάνει να βρίσκει σχεδόν πάντα με επιτυχία την αναζήτηση του χρήστη.

Η εφαρμογή είναι διαθέσιμη για τα λειτουργικά συστήματα Windows, iOS, Android και Linux. Μετά την εγκατάσταση της εφαρμογής, ο χρήστης εγγράφεται μέσω Facebook ή email. Στην εφαρμογή, υπάρχει και η δυνατότητα του Επισκέπτη (Guest User) όπου ο χρήστης δεν κάνει εγγραφή και έτσι δεν παραχωρεί τα προσωπικά του δεδομένα, όμως δεν επωφελείται και όλες τις λειτουργίες αυτής. Η παραχώρηση προσωπικών δεδομένων του χρήστη σε συνδυασμό με την υψηλή απήχηση που έχει η συγκεκριμένη εφαρμογή οδήγησαν την συγγραφέα στη μελέτη της πολιτικής ιδιωτικότητας της. [\[28\]](#)

➤ **Πληροφορίες που Συλλέγει η Εφαρμογή**

- Προσωπικές πληροφορίες οι οποίες δίδονται από το χρήστη κατά τη δημιουργία του λογαριασμού του, όπως email, κωδικό πρόσβασης. Επίσης, χρησιμοποιούνται σε περίπτωση ανάκτησης του λογαριασμού καθώς και για επικοινωνία και υποστήριξη από την εξυπηρέτηση πελατών. Τα στοιχεία

αποθηκεύονται στους servers του Stremio όμως βρίσκονται σε ασφαλή και κρυπτογραφημένη μορφή.

- Πληροφορίες όπως διεύθυνση IP, λειτουργικό σύστημα, γλώσσα, μοναδικό χαρακτηριστικό συσκευής, μέρα και ώρα χρήσης της εφαρμογής. Τα χαρακτηριστικά αυτά, στη “γλώσσα” των εφαρμογών ονομάζονται Log Information.
- Δεδομένα τα οποία η εφαρμογή λαμβάνει από τρίτες οντότητες όπως για παράδειγμα όταν ο χρήστης συνδεθεί μέσω Facebook, η εφαρμογή αυτόματα αποκτά πρόσβαση στις προσωπικές πληροφορίες του χρήστη στο Facebook. Τρίτες οντότητες όπως το Facebook μπορεί να είναι το Play Store ή το iTunes.
- Δεδομένα τα οποία χρησιμοποιούνται για σκοπούς έρευνας και ανάλυσης κοινού. Το Stremio διαθέτει τους δικούς της αναλυτές, Google Analytics και BigQuery, για την συγκέντρωση και συλλογή των δεδομένων, προκειμένου να βελτιωθεί η απόδοση και η ποιότητα της εφαρμογής. Οι τρίτες οντότητες που χρησιμοποιεί το Stremio ακολουθούν τις βέλτιστες πρακτικές προστασίας δεδομένων και τηρούν τους πιο πρόσφατους νόμους.

➤ **Γνωστοποίηση των Πληροφοριών με Τρίτες Οντότητες**

- Μεταφορά των προσωπικών δεδομένων του χρήστη σε τρίτους για την παροχή υπηρεσιών, για παράδειγμα όσον αφορά αιτήματα που έχει υποβάλει ο χρήστης.
- Οι τρίτοι πάροχοι ωστόσο, δεν έχουν καμία εξουσιοδότηση να διατηρούν, μοιράζονται ή αποθηκεύουν τα στοιχεία αυτά, για άλλους σκοπούς πέρα από την παροχή των υπηρεσιών που έχουν προσληφθεί να παρέχουν.
- Το Stremio δεν έχει δικαιοδοσία να πουλήσει, ανταλλάξει ή μοιράσει με άλλο τρόπο τις προσωπικές πληροφορίες των χρηστών.

➤ **Χρήση των Δεδομένων**

- Παροχή υπηρεσιών.
- Βελτιστοποίηση των διαφημίσεων.
- Ενημέρωση χρήστη σχετικά με νέες υπηρεσίες.
- Παρακολούθηση της χρήσης των υπηρεσιών και πρόβλεψη αναδυόμενων τάσεων.
- Παροχή εξατομικευμένων διαφημίσεων, μόνο με τη συγκατάθεση του χρήστη.

(Ημερομηνία τελευταίας αναθεώρησης πολιτικής ιδιωτικότητας Stremio: 30 Αυγούστου 2020)

7. Google Chrome

Το Google Chrome αποτελεί τον πιο δημοφιλή περιηγητή ξεπερνώντας αυτό των Windows που για αρκετά χρόνια βρισκόταν στην

κορυφή.[\[29\]](#) Η επίσημη έκδοση κυκλοφόρησε τον Δεκέμβριο του 2008 και σήμερα οι χρήστες του Google Chrome ανέρχονται σε αριθμό μεγαλύτερο του ενός δισεκατομμυρίου. Η μεγάλη ζήτηση της συγκεκριμένης εφαρμογής συνέβαλε στην έρευνα και σχολιασμό της πολιτικής ιδιωτικότητας της. [\[30\]](#)

Παρατηρώντας την πολιτική ιδιωτικότητας του Google Chrome διακρίνει κανείς ότι υπάρχουν διαφορετικές λειτουργίες περιήγησης ανάλογα με τις ανάγκες του χρήστη. Αυτές οι λειτουργίες αποτελούνται από:

- Την **βασική** λειτουργία περιήγησης (Basic Browser Mode).
- Την λειτουργία **σύνδεσης** και **συγχρονισμού** (Sign-in & Sync Mode).
- Την λειτουργία **ανώνυμης** περιήγησης και λειτουργία **επισκέπτη** (Incognito and Guest Mode).

- Στη βασική λειτουργία (basic browser mode) οι πληροφορίες δεν αποθηκεύονται στους servers της Google αλλά στη συσκευή του χρήστη.

Οι πληροφορίες αποτελούνται από :

- Ιστορικό περιήγησης όπως για παράδειγμα τις διευθύνσεις URL που επισκέφθηκε ο χρήστης, εικόνες και προσωρινό κείμενο. Εάν η λειτουργία πρόβλεψης ενεργειών δικτύου είναι ενεργοποιημένη από τις ρυθμίσεις, το Google Chrome αποθηκεύει και ορισμένες διευθύνσεις IP που συνδέονται με τις σελίδες που επισκέφθηκε.
- Προσωπικές πληροφορίες όπως όνομα και κωδικό, οι οποίες παραχωρούνται κατά την εγγραφή και χρησιμοποιούνται κατά την είσοδο.
- Cookies.
- Ιστορικό λήψεων.

Οι πληροφορίες αυτές αποθηκεύονται στους Servers του Google Chrome μόνο αν επιλέξει ο χρήστης το συγχρονισμό τους με το Google. Στην περίπτωση που τα δεδομένα αφορούν λογαριασμούς τραπεζών και πληροφορίες πιστωτικής κάρτας, αυτά δεν αποθηκεύονται στο λογαριασμό Google Payment εφόσον δεν παραχωρηθεί η άδεια από το χρήστη.

- Στη λειτουργία συγχρονισμού (Sync mode), τα προσωπικά δεδομένα του χρήστη αποθηκεύονται στους Servers του Google Chrome έτσι ώστε ο χρήστης να μπορεί να έχει πρόσβαση σε αυτά όταν συνδέεται και συγχρονίζεται με το Google Chrome σε άλλους υπολογιστές ή συσκευές. Οι πληροφορίες περιλαμβάνουν :

- Ιστορικό χρήστη
- Σελιδοδείκτες
- Καρτέλες

- Κωδικοί και αυτόματη συμπλήρωση
- Άλλες ρυθμίσεις του περιηγητή, όπως οι πρόσθετες υπηρεσίες.

Ο χρήστης έχει τη δυνατότητα οποιαδήποτε στιγμή να διαχειριστεί το συγχρονισμένο του λογαριασμό, να σβήσει δεδομένα και να προσαρμόσει τις ανάγκες του μέσω των ρυθμίσεων.

- Στη λειτουργία ανώνυμης περιήγησης, οι πληροφορίες οι οποίες αποθηκεύονται είναι ελάχιστες γι' αυτό και πολλοί χρήστες επιλέγουν αυτή τη λειτουργία. Οι πληροφορίες που δεν συλλέγονται είναι οι εξής :
 - Βασικές πληροφορίες όπως ιστορικό περιήγησης, διευθύνσεις URL, κρυφή μνήμη κειμένου σελίδας, διευθύνσεις IP.
 - Στιγμιότυπα σελίδων.
 - Στοιχεία λήψεων, παρόλο που τα αρχεία αποθηκεύονται στη συσκευή.

Συγκεκριμένες πληροφορίες όπως cookies, πληροφορίες προφίλ κ.α. αποθηκεύονται κατά τη διάρκεια της περιήγησης, όμως σβήνονται με το κλείσιμο του ανώνυμου περιηγητή, και δεν χρησιμοποιούνται από την εφαρμογή.

➤ **Τρόπος Χρήσης των Δεδομένων**

- Οι ιστότοποι που επισκέπτεται ο χρήστης μέσω του Google Chrome λαμβάνουν αυτόματα πληροφορίες όπως διεύθυνση IP και Cookies. Αν ο Google Chrome αντιληφθεί κάποια κακόβουλη επίθεση σε ένα δίκτυο, τότε στέλνει πληροφορίες για αυτήν τη σύνδεση στο Google έτσι ώστε να προσδιορίσει την επίθεση.
- Ο Google Chrome δίνει την επιλογή στο χρήστη να μοιρασθεί την τοποθεσία του με τις ιστοσελίδες που χρησιμοποιεί, για περισσότερες γεωγραφικές πληροφορίες, όμως, δεν το επιτρέπει χωρίς την άδεια του χρήστη. Ωστόσο, σε λογισμικό Android, εφόσον ο χρήστης δώσει το δικαίωμα της τοποθεσίας από τις ρυθμίσεις της εφαρμογής αυτή μπορεί να παραχωρήσει αυτοματοποιημένα την τοποθεσία του χρήστη σε όλες τις ιστοσελίδες χωρίς την πληροφόρηση του.
- Η εφαρμογή διαθέτει τη λειτουργία Google Location Service με την οποία υπολογίζει την τοποθεσία του χρήστη κάνοντας χρήση τα κοντινά Wi-Fi router και την διεύθυνση IP της συσκευής.
- Για τις ενημερώσεις του λογισμικού, το Google Chrome αποστέλλει πληροφορίες όπως την κατάσταση σύνδεσης, την ώρα καθώς και τον αριθμό των συνδεδεμένων χρηστών.

- Για την αυτοματοποιημένη συμπλήρωση των στοιχείων πρόσβασης(username, password), στέλνονται στην Google οι χαρακτήρες που έχει πληκτρολογήσει ήδη ο χρήστης και βάση του ιστορικού αναζήτησης η Google προβλέπει τα στοιχεία αυτά.
- Το Google Chrome αποστέλλει αυτοματοποιημένα στατιστικά στοιχεία χρήσης και αναφορές ασφαλιμάτων με στόχο τη βελτίωση των υπηρεσιών του. Τα στατιστικά στοιχεία χρήσης περιλαμβάνουν πληροφορίες όπως προτιμήσεις, κλικ, στατιστικά απόδοσης και χρήση μνήμης. Στην λειτουργία συγχρονισμού, περιλαμβάνονται και άλλα στοιχεία όπως ιστορικό χρήστη, φύλο, ηλικία και άλλα δημογραφικά στοιχεία.

*(Ημερομηνία τελευταίας αναθεώρησης πολιτικής
Ιδιωτικότητας Google Chrome: Μάιος 2020)*

8. Mozilla Firefox

Ο Mozilla Firefox αποτελεί τον δεύτερο πιο διαδεδομένο περιηγητή με χιλιάδες εκατομμύρια λήψεις το χρόνο. [\[31\]](#) Η κυκλοφορία του έγινε τον Σεπτέμβριο του 2002 και με κάποιες αλλαγές ονομάτων κατέληξε στην τελική ονομασία Mozilla Firefox ή αλλιώς Fx. Οι λήψεις της εφαρμογής στο Play Store αγγίζει τα 500 εκατομμύρια στο Market του Android και λόγω της δημοτικότητας της είναι απαραίτητο να ερευνηθεί η πολιτική ιδιωτικότητας της.

Η εφαρμογή Mozilla Firefox συλλέγει τα δεδομένα του χρήστη από :

- Τον ίδιο το χρήστη για παράδειγμα όταν αποστέλλει αναφορά σφάλματος.
- Αυτομάτως μέσω των προϊόντων και υπηρεσιών του Mozilla.
- Τρίτες οντότητες με τις οποίες συνεργάζεται η εφαρμογή όπως για παράδειγμα η Thunderbird.
- Βάση πληροφοριών που έχει δώσει ο χρήστης, το Mozilla προσπαθεί να κατανοήσει περισσότερα για τις ανάγκες του χρήστη έτσι ώστε να εξατομικεύσει την εμπειρία της περιήγησης του.

➤ Χρήση και Κοινοποίηση των Δεδομένων

Το Mozilla Firefox χρησιμοποιεί τις πληροφορίες μόνο με τρόπους για τους οποίους ο χρήστης έχει παραχωρήσει άδεια και έχοντας ως σκοπό τη βελτίωση της εμπειρίας του χρήστη. Η εφαρμογή του Mozilla δεσμεύεται για την προστασία και ασφάλεια των δεδομένων και διατηρεί τα στοιχεία για όσο τα χρειάζεται και στη συνέχεια τα διαγράφει.

Οι πληροφορίες χρησιμοποιούνται για τους παρακάτω σκοπούς :

- Για την επεξεργασία και παροχή προϊόντων και υπηρεσιών στο χρήστη, αλλά μόνο εάν οι οντότητες που λαμβάνουν τις πληροφορίες συμμορφώνονται με τις πολιτικές της εφαρμογής Mozilla.
- Ορισμένες φορές το Mozilla, κοινοποιεί πληροφορίες με στόχο τη βελτίωση των προϊόντων του. Ωστόσο, όταν γίνει αυτό αποφεύγεται η κοινοποίηση των προσωπικών στοιχείων των χρηστών.
- Όταν ο νόμος ή η κυβέρνηση το επιβάλλουν, η εφαρμογή του Mozilla είναι αναγκασμένη να παραχωρήσει προσωπικά δεδομένα.
- Για την ασφάλεια και προστασία του χρήστη από παράνομες ή κακόβουλες επιθέσεις.
- Σε περίπτωση μεταβίβασης ή χρεοκοπίας της εταιρείας, τα δεδομένα θα διαβιβαστούν στην ανάδοχη εταιρεία.

Κατά τη μελέτη της πολιτικής ιδιωτικότητας του Mozilla Firefox ωστόσο, παρατηρήθηκε πως αναφέρεται ότι λόγω του ότι η εφαρμογή αποτελεί παγκόσμια εταιρεία, με έδρες σε πολλές χώρες, υπάρχει η πιθανότητα τα προσωπικά δεδομένα των χρηστών να καταλήξουν σε ηλεκτρονικούς υπολογιστές άλλων χωρών από ότι του χρήστη. Η δήλωση αυτή ελλοχεύει κινδύνους καθώς, κάθε χώρα διαθέτει διαφορετικά επίπεδα προστασίας των προσωπικών δεδομένων με αποτέλεσμα την διακύβευση της ασφάλειας του χρήστη.

*(Ημερομηνία τελευταίας αναθεώρησης πολιτικής
Ιδιωτικότητας Mozilla Firefox: 8 Σεπτεμβρίου 2020)*

9.Skype

Το Skype αποτελεί μια εξαιρετική εφαρμογή τύπου VoIP, προσφέροντας τηλεφωνία μέσω διαδικτύου. [32] Αρχικά, το Skype διέθετε επικοινωνία αποκλειστικά μεταξύ υπολογιστών. Πλέον όμως, παρέχει κλήσεις σε οποιοδήποτε μέρος του κόσμου, με οποιοδήποτε δίκτυο τηλεφωνίας, σταθερής και κινητής, Instant Messenger, SMS, με δυνατότητα αποστολής αρχείων και συνδιάσκεψης, με πολλά άτομα ταυτόχρονα. Οι υπηρεσίες που προσφέρονται στο χρήστη είναι απεριόριστες και σε αυτό οφείλονται οι εκατομμύρια λήψεις στο Play Store. Η εφαρμογή κυκλοφόρησε το 2003 και διατίθενται σε εκδόσεις για Mac, Linux, Windows, Android, iOS, ακόμα και για κονσόλες βιντεοπαιχνιδιών όπως Xbox One και Microsoft.

Η εφαρμογή Skype ανήκει στον όμιλο της Microsoft και γι' αυτό το λόγο θα μελετηθεί η πολιτική ιδιωτικότητας της Microsoft. [33] [34]

➤ Προσωπικά Δεδομένα που Συλλέγει η Εφαρμογή

- Η Microsoft συλλέγει δεδομένα από το χρήστη, μέσω της αλληλεπίδρασης του με τα προϊόντα της.

- Ορισμένα προσωπικά δεδομένα του χρήστη τα παρέχει ο ίδιος ο χρήστης, κάποια τα συλλέγει η Microsoft μέσω της αλληλεπίδρασης, της χρήσης και της εμπειρίας του χρήστη με τα προϊόντα. Τα δεδομένα που συλλέγει η εφαρμογή εξαρτώνται από τις επιλογές του χρήστη και τις ρυθμίσεις απορρήτου.
- Επίσης, η εφαρμογή αποκτά ορισμένα δεδομένα μέσω τρίτων οντοτήτων.
- Ο χρήστης μπορεί να επιλέξει να μην παρέχει τα προσωπικά του δεδομένα στη Microsoft, ωστόσο δεν θα είναι σε θέση να χρησιμοποιήσει το προϊόν το οποίο ζητούσε την παροχή των πληροφοριών αυτών.

➤ **Χρήση των Δεδομένων**

Η Microsoft, και κατά συνέπεια το Skype χρησιμοποιούν τα προσωπικά δεδομένα των χρηστών ως εξής:

- Για την παροχή προϊόντων και την ενημέρωση του χρήστη σχετικά με αυτά.
- Για την διασφάλιση, την αντιμετώπιση προβλημάτων και την άμεση παροχή υποστήριξης από την εξυπηρέτηση πελατών.
- Για την κοινοποίηση δεδομένων, όταν αυτό απαιτείται για την παροχή μιας υπηρεσίας ή για την εκτέλεση των αιτούμενων συναλλαγών.
- Για τη βελτίωση και ανάπτυξη των προϊόντων της.
- Για την εξατομίκευση της εμπειρίας του χρήστη .
- Για διαφημιστικούς σκοπούς, όπου περιλαμβάνεται αποστολή διαφημιστικού υλικού και προβολή σχετικών προσφορών .
- Για την ανάλυση των επιδόσεων της εφαρμογής, την ανάπτυξη του εργατικού δυναμικού και την διεξαγωγή ερευνών .
- Κατά τη διεξαγωγή των ερευνών, η Microsoft συνδυάζει δεδομένα του χρήστη, για παράδειγμα από δυο προϊόντα της Microsoft που ο ίδιος χρησιμοποιεί, για την παροχή ομαλής και εξατομικευμένης εμπειρίας.
- Η επεξεργασία των προσωπικών δεδομένων για τους παραπάνω σκοπούς, περιλαμβάνει αυτοματοποιημένες αλλά και μη αυτόματες μεθόδους επεξεργασίας. Για παράδειγμα, αυτοματοποιημένη επεξεργασία θεωρείται η τεχνητή νοημοσύνη με την οποία οι υπολογιστές εκπαιδεύονται να αντιλαμβάνονται, να μαθαίνουν και να λαμβάνουν αποφάσεις για την επίλυση προβλημάτων. Για την εκπαίδευση και την ακρίβεια των αυτοματοποιημένων μεθόδων, όπως η τεχνητή νοημοσύνη, υπάρχουν μη αυτόματες μέθοδοι όπου άνθρωποι παρακολουθούν την εξέλιξη των αυτοματοποιημένων μεθόδων, μελετώντας τις προβλέψεις και τα συμπεράσματα που προκύπτουν. Έτσι για παράδειγμα, η Microsoft ελέγχει με μη αυτόματο τρόπο μικρά αποσπάσματα φωνητικών δεδομένων, αφαιρώντας τα προσωπικά στοιχεία, προκειμένου να βελτιώσει τις υπηρεσίες φωνητικών εντολών, όπως η αναγνώριση και η μετάφραση.

➤ **Γνωστοποίηση των Πληροφοριών σε Τρίτες Οντότητες**

- ο Κοινοποίηση των προσωπικών δεδομένων του χρήστη με την συγκατάθεση του ιδίου.
- ο Για την ολοκλήρωση οποιασδήποτε συναλλαγής ή την παροχή οποιουδήποτε προϊόντος.
- ο Κοινοποίηση δεδομένων σε συγγενείς ή και θυγατρικές εταιρείες της Microsoft.
- ο Παροχή πληροφοριών σε προμηθευτές που συνεργάζονται με την Microsoft.
- ο Κοινοποίηση προσωπικών δεδομένων όταν το απαιτεί ο νόμος ή η κυβέρνηση.
- ο Όταν αφορά την προστασία των χρηστών, την διατήρηση της ασφάλειας των προϊόντων, των δικαιωμάτων και ιδιοκτησίας της Microsoft.

*(Ημερομηνία τελευταίας αναθεώρησης πολιτικής
Ιδιωτικότητας Skype: Σεπτέμβριος 2020)*

10.Zoom

Η εφαρμογή Zoom, όπως και το Skype το οποίο αναλύσαμε νωρίτερα αποτελεί ένα πρόγραμμα τηλεδιάσκεψης, το οποίο παρέχει στο χρήστη υπηρεσία βίντεο κλήσης με έως και εκατό συσκευές ταυτόχρονα με χρονικό περιορισμό σαράντα λεπτών. Στην περίπτωση όπου ο χρήστης αναβαθμίσει την εμπειρία του έναντι χρημάτων, του παρέχεται η δυνατότητα να δημιουργήσει βίντεο κλήσεις μεταξύ χιλίων ατόμων και δίχως χρονικό περιορισμό.

Με την εμφάνιση της πανδημίας Covid-19, η εφαρμογή Zoom σημείωσε ραγδαία αύξηση χρήσης, με σκοπό την απομακρυσμένη εργασία, την εξ αποστάσεως εκπαίδευση αλλά και την καθημερινή χρήση μεταξύ συγγενών και φίλων. Την εφαρμογή του Zoom, τον Απρίλιο του 2020 χρησιμοποιούσαν περισσότεροι από 300 εκατομμύρια χρήστες καθημερινά.

Η πολιτική ιδιωτικότητας της εφαρμογής, παρουσιάζει εμπεριστατωμένα τις πληροφορίες τις οποίες συλλέγει, το πως συλλέγονται και με ποιόν σκοπό . [\[35\]](#)

➤ **Πληροφορίες που Συλλέγει το Zoom**

- ο Στην δωρεάν έκδοση της εφαρμογής Zoom συλλέγονται οι πληροφορίες που παρέχει ο χρήστης κατά την εγγραφή του στην εφαρμογή, όπως ημερομηνία γέννησης, ονοματεπώνυμο, τηλέφωνο, email, γλώσσα, User ID, password, φωτογραφία προφίλ και πρόγραμμα συναντήσεων.
- ο Στην έκδοση επί πληρωμή, εκτός από τις παραπάνω πληροφορίες λογαριασμού, τα δεδομένα που καταχωρούνται

- αφορούν πληροφορίες πληρωμής, όπως όνομα, τηλέφωνο, διεύθυνση χρέωσης καθώς και τρόπο πληρωμής.
- Τεχνικές πληροφορίες σχετικά με το λογισμικό που φιλοξενεί τις υπηρεσίες του Zoom αλλά και μετρήσεις σχετικές με τον τρόπο και το χρόνο διεξαγωγής των συσκέψεων.
 - Δεδομένα απόδοσης, μετρήσεις και πληροφορίες κατάστασης συστήματος.
 - Κατά προσέγγιση τοποθεσία.
 - Διεύθυνση IP, τύπος προγράμματος περιηγητή, αρχεία που προβάλλονται στους ιστοτόπους μάρκετινγκ(για παράδειγμα σελίδες HTML, γραφικά κ.α.), λειτουργικό σύστημα, ημερομηνία και ώρα σύσκεψης.
 - Οι πληροφορίες που συλλέγονται μέσω των Cookies, οι οποίες είναι απαραίτητες για τεχνική υποστήριξη και παροχή υπηρεσιών.
 - Ορισμένες φορές παρέχονται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου των χρηστών σε τρίτες οντότητες, για λόγους marketing.
 - Όσον αφορά εκδηλώσεις οι οποίες έχουν χορηγηθεί από το Zoom (Sponsored), η εφαρμογή συλλέγει πληροφορίες όπως τον τίτλο του event, το email, τον εργοδότη και τον τίτλο εργασίας, εάν υπάρχουν.

➤ **Τρόπου Συλλογής των Δεδομένων**

Η εφαρμογή συλλέγει τα προσωπικά δεδομένα των χρηστών με τους εξής τρόπους:

- Κατά την δωρεάν εγγραφή του χρήστη στην εφαρμογή.
- Κατά την πληρωμένη εγγραφή του χρήστη στην εφαρμογή.
- Ορισμένες πληροφορίες καταχωρούνται αυτομάτως μέσω της χρήσης των υπηρεσιών του Zoom.
- Μέσω των Cookies, ανάλογα την διαμόρφωση του εργαλείου προτιμήσεων Cookies από το χρήστη.
- Μέσω τρίτων οντοτήτων και δημοσίων πηγών.

➤ **Τρόπος Χρήσης των Δεδομένων**

Σύμφωνα με την πολιτική ιδιωτικότητας της, η εφαρμογή Zoom χρησιμοποιεί τα δεδομένα που συλλέγει για κάποιους από τους παρακάτω σκοπούς:

- Εγγραφή του χρήστη στις υπηρεσίες.
- Εμφάνιση του User Avatar του χρήστη στους συμμετέχοντες κατά τη σύσκεψη.
- Παροχή υποστήριξης πελατών.
- Αποστολή ανακοινώσεων στο χρήστη που αφορούν αναβαθμίσεις και βελτιώσεις του συστήματος, ενημερώσεις λογισμικού και διαφημίσεις.

- Εκτέλεση διαγωνισμών συμμετοχής, κληρώσεων και λοιπών διαφημιστικών δραστηριοτήτων.
- Διατήρηση της ασφάλειας του χρήστη καθώς και των υπηρεσιών του Zoom.
- Διερεύνηση και διακοπή παράνομων και μη εξουσιοδοτημένων δραστηριοτήτων.
- Δημιουργία ανώνυμων ή/και συγκεντρωτικών αναλυτικών στοιχείων για τη βελτίωση των προϊόντων της εφαρμογής.
- Προσδιορισμός των γλωσσικών προτιμήσεων, ολοκλήρωση των παραγγελιών και μνημόνευση των ρυθμίσεων του χρήστη.

(Ημερομηνία τελευταίας αναθεώρησης πολιτικής
Ιδιωτικότητας Zoom: Αύγουστος 2020)

4.4 Αποτελέσματα και Συγκρίσεις από τη Μελέτη των Πολιτικών Ιδιωτικότητας των Δέκα πιο Επιτυχημένων Εφαρμογών

○ Facebook

Μελετώντας την πολιτική ιδιωτικότητας του Facebook απαριθμούμε δεκάδες άδειες οι οποίες ζητούνται από το χρήστη, κάποιες από τις οποίες ορίζονται ως επικίνδυνες. Γίνεται συλλογή επικίνδυνων αδειών όπως πληροφορίες κάμερας, ιστορικό κλήσεων και SMS, σημάτων Bluetooth κ.α. Το Facebook συλλέγει πολλές πληροφορίες από τη συσκευή του χρήστη αλλά και αρκετές από τρίτες οντότητες και συνεργαζόμενες επιχειρήσεις.

Ωστόσο, στην πολιτική ιδιωτικότητας της εφαρμογής, αναφέρονται οι σκοποί για τους οποίους συλλέγονται τα δεδομένα προάγοντας την διαφάνεια και την ειλικρίνεια προς το χρήστη.

Συμπερασματικά, η εφαρμογή Facebook αντλεί μεγάλο πλήθος προσωπικών δεδομένων και επικίνδυνων αδειών παρόλα αυτά ορίζει τους τρόπους χρήσης και διαχείρισης των δεδομένων, γεγονός που καθιστά την πολιτική ιδιωτικότητας της, σαφή και πλήρη.

-Read Call Log, -Read Contacts, -Read SMS	Ιστορικό Κλήσεων, Κατάλογος Επαφών, Ιστορικό Μηνυμάτων	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αν ο χρήστης επιθυμεί
Modify System Settings, -Read Battery Statistics	Λειτουργικό σύστημα, Πληροφορίες συστήματος, Επίπεδο μπαταρίας	Αναφέρεται στην πολιτική ιδιωτικότητας/Αντλούνται αυτοματοποιημένα από την εφαρμογή.

-Wi-Fi Connections, -View Network Connections, -Access Bluetooth Settings, -Pair Bluetooth Devices	Σημεία Πρόσβασης Διαδικτύου, Πύργους Κινητής Τηλεφωνίας, Σήματα Bluetooth	Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αυτοματοποιημένα από την εφαρμογή.
-Read Storage -Write Storage -Access Camera -Access Coarse Location -Access Fine Location	Πρόσβαση σε : Αποθηκευτικό χώρο, Φωτογραφίες, Τοποθεσία	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αν ο χρήστης επιθυμεί.
-Read Calendar -Record Audio	Ημερολόγιο, Εγγραφή Ήχου	Επικίνδυνες Άδειες. Η άντληση και χρήση τους δεν αναφέρονται στην πολιτική ιδιωτικότητας.

Πίνακας 10. Δεδομένα που αντλεί η εφαρμογή Facebook.

ο **Twitter**

Η εφαρμογή Twitter παρουσιάζει αρκετές ελλείψεις στην πολιτική ιδιωτικότητας της. Γίνεται αναφορά για τη συλλογή των πληροφοριών λογαριασμού και επικοινωνίας του χρήστη όμως παραλείπεται η αναφορά στη συλλογή δεδομένων που αφορούν επικίνδυνες άδειες όπως κάμερα, μικρόφωνο κ.α.

Παράλληλα, το Twitter δεν γνωστοποιεί τους τρόπους χρήσης και διαχείρισης των δεδομένων που συλλέγει, αφήνοντας τους χρήστες της σε πλήρη άγνοια των σκοπών του.

Καταλήγουμε στο συμπέρασμα πως η πολιτική ιδιωτικότητας του Twitter θεωρείται ανεπαρκής αφού η εφαρμογή επιλέγει να παραλείψει σημαντικά ζητήματα που απειλούν την ασφάλεια του χρήστη .

-Access Fine Location -Access Coarse Location	Τοποθεσία	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Λαμβάνεται αυτόματα από την εφαρμογή.
-Receive Data from Internet	Πληροφορίες Πιστωτικής/Χρεωστικής Κάρτας, Ιστότοποι που επισκέπτεται ο χρήστης	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αυτόματα από την εφαρμογή

-Read Phone State	Πληροφορίες τηλεφώνου, Κατάσταση Κινητού τηλεφώνου	Αναφέρεται στην πολιτική ιδιωτικότητας ως προαιρετικό / Αντλείται αυτόματα από την εφαρμογή χωρίς την συγκατάθεση του χρήστη.
-Read Storage, -Write Storage, -Access Camera, -Record Audio, -Read Contacts	-Αποθηκευτικός χώρος, -Φωτογραφίες, Κάμερα, -Μικρόφωνο, -Επαφές	Επικίνδυνες Άδειες. Η άντληση και χρήση τους δεν αναφέρονται στην πολιτική ιδιωτικότητας.

Πίνακας 11. Δεδομένα που αντλεί η εφαρμογή Twitter.

ο **Facebook & Twitter**

Συγκρίνοντας τις εφαρμογές κοινωνικής δικτύωσης Facebook και Twitter ως προς τις πολιτικές ιδιωτικότητας τους, παρατηρούμε ότι παρόλο που το Facebook συλλέγει μεγαλύτερο όγκο προσωπικών δεδομένων, το Twitter αδυνατεί να γνωστοποιήσει ορισμένα δεδομένα που συλλέγει αλλά και τον τρόπο και σκοπό χρήση τους. Συνεπώς, η πολιτική ιδιωτικότητας της εφαρμογής Facebook κρίνεται πιο ολοκληρωμένη και διαφανής προς τους χρήστες της, από το Twitter.

ο **Viber**

Η πολιτική ιδιωτικότητας της εφαρμογής Viber παρουσιάζεται αρκετά αναλυτική ως προς πληροφορίες που συλλέγει. Τα δεδομένα των χρηστών αποθηκεύονται, όμως δεν διαβάζονται και διαγράφονται από τους Servers όταν ο χρήστης απενεργοποιήσει το λογαριασμό του.

Παράλληλα αναφέρονται με σαφήνεια οι τρόποι χρήσης των προσωπικών δεδομένων που έχουν αντληθεί από την εφαρμογή.

Ωστόσο η αδυναμία που εντοπίστηκε είναι πως ο διαμοιρασμός των πληροφοριών σε τρίτες οντότητες δεν αναλύεται εκτενώς.

-Create Accounts, -Set Passwords, -Add/Remove Accounts	Δημιουργία και πληροφορίες λογαριασμού	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται από το χρήστη κατά τη δημιουργία λογαριασμού.
--	--	---

-Read Contacts, -Read Phone Status	Πληροφορίες επαφών και κινητού τηλεφώνου	Αναφέρεται στην πολιτική ιδιωτικότητας/Αντλούνται αν ο χρήστης επιθυμεί
-Read Data from Internet	Πληροφορίες από τρίτες οντότητες	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αν ο χρήστης συνδεθεί μέσω του Viber σε τρίτες οντότητες όπως Facebook ,Twitter.
-Modify System Settings -View Wi-Fi Connections -View Network Connections	Πληροφορίες λειτουργικού συστήματος, Σημεία Πρόσβασης Διαδικτύου, Πύργους Κινητής Τηλεφωνίας	Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αυτόματα από την εφαρμογή.
-Access Fine Location -Access Coarse Location	Τοποθεσία	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αν ο χρήστης το επιθυμεί.

Πίνακας 12. Δεδομένα που αντλεί η εφαρμογή Viber.

ο **WhatsApp**

Η πολιτική ιδιωτικότητας της εφαρμογής WhatsApp παρουσιάζεται επίσης εμπεριστατωμένη και σαφής προς το χρήστη, με ελάχιστες ελλείψεις.

Υπάρχει σχεδόν πλήρης αναφορά ως προς τα δεδομένα που συλλέγει, εκτός από την πρόσβαση στα μηνύματα της συσκευής. Σύμφωνα με την πολιτική απορρήτου της εφαρμογής WhatsApp, όλα τα δεδομένα οπτικοακουστικού υλικού αλλά και αρχεία, διαγράφονται μετά την επιτυχημένη αποστολή τους στον παραλήπτη.

Η πολιτική ιδιωτικότητας του WhatsApp παρέχει πλήρης επεξήγηση ως προς τους σκοπούς συλλογής των προσωπικών δεδομένων των χρηστών αλλά και επαρκής αναφορά στην κοινοποίηση δεδομένων σε τρίτες οντότητες.

-Add Accounts -Remove Accounts -Find Accounts	Δημιουργία και πληροφορίες λογαριασμού	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Παίρνονται όλες οι επαφές του χρήστη , και αυτές που δεν διαθέτουν WhatsApp.
---	--	---

-Modify System Settings -Read Battery Statistics	Πληροφορίες Λειτουργικού Συστήματος, Επίπεδο Μπαταρίας	Αναφέρονται στην πολιτική ιδιωτικότητας/ Αντλούνται αυτοματοποιημένα από την εφαρμογή.
-Read Phone Status	Πληροφορίες κινητής συσκευής, Δίκτυο Κινητής τηλεφωνίας, Διεύθυνση IP	Αναφέρονται στην πολιτική ιδιωτικότητας/ Αντλούνται αυτοματοποιημένα από την εφαρμογή.
-View Wi-fi Connections -Access Fine Location -Access Coarse Location -Pair with Bluetooth Devices	GPS, Bluetooth, Σημεία Πρόσβασης Διαδικτύου, Τοποθεσία	Αναφέρονται στην πολιτική ιδιωτικότητας/Αντλούνται με την έγκριση του χρήστη .
-Access Camera -Read Storage -Write Storage -Record Audio -Read Contents of Storage	Πρόσβαση σε: Κάμερα, Αποθηκευτικό Χώρο, Μικρόφωνο	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας πως μόλις σταλούν επιτυχώς στον παραλήπτη , διαγράφονται από τους servers της εταιρείας.
-Receive SMS -Send SMS	Μηνύματα	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας.

Πίνακας 13. Δεδομένα που αντλεί η εφαρμογή WhatsApp.

○ **Viber & WhatsApp**

Συγκρίνοντας τις δυο παρόμοιες εφαρμογές άμεσης ανταλλαγής μηνυμάτων Viber και WhatsApp, παρατηρούμε παρόμοιες προσεγγίσεις πολιτικών απορρήτου. Οι δυο εφαρμογές διαθέτουν ορισμένες ελλείψεις στον τομέα της συλλογής πληροφοριών, όμως παρουσιάζουν μεγάλη ανάλυση ως προς τον τρόπο χρήσης των δεδομένων. Κρίνοντας από την ανάλυση που έγινε, η πολιτική ιδιωτικότητας της εφαρμογής WhatsApp μπορεί να θεωρηθεί πιο επεξηγηματική και σαφής καθώς, αναλύει τις πληροφορίες που διαμοιράζεται με τις τρίτες οντότητες, σε αντίθεση με το Viber.

○ **Netflix**

Η πολιτική ιδιωτικότητας του Netflix παρουσιάστηκε πολύ επεξηγηματική και αναλυτική ως προς τα δεδομένα που συλλέγει αλλά και τις πηγές από τις οποίες τα αντλεί. Ορισμένες πληροφορίες παρέχονται απευθείας από το χρήστη, άλλες αντλούνται αυτοματοποιημένα και κάποιες άλλες μέσω συνεργατών και άλλων πηγών.

Παράλληλα, στην πολιτική ιδιωτικότητας αναφέρονται οι σκοποί και τρόποι χρήσης των δεδομένων που συλλέγονται και κατηγοριοποιούνται οι τρίτες οντότητες στις οποίες κοινοποιούνται προσωπικά δεδομένα των χρηστών.

Διαβάζοντας τους όρους απορρήτου της εφαρμογής Netflix καταλήγουμε στο συμπέρασμα ότι πρόκειται για μια αναλυτική και ολοκληρωμένη πολιτική ιδιωτικότητας, με σαφήνεια και διαφάνεια προς το χρήστη.

-Add Accounts -Remove Accounts	Πληροφορίες και δημιουργία λογαριασμού	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται από το χρήστη κατά τη δημιουργία λογαριασμού.
-Read Phone Status	Κινητό Τηλέφωνο, Αναγνωριστικά Συσκευής	Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται Αυτοματοποιημένα Από την εφαρμογή.
-Modify System Settings -View Wi-fi Connections -Access Fine Location -Access Coarse Location	Πληροφορίες Λειτουργικού Συστήματος, Διεύθυνση IP, Σημεία Πρόσβασης Διαδικτύου, Τοποθεσία	Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αυτοματοποιημένα από την εφαρμογή.
-Access Storage -Record Audio	Αποθηκευτικός χώρος, Μικρόφωνο	Επικίνδυνες Άδειες. Δεν αναφέρονται στην πολιτική ιδιωτικότητας.

Πίνακας 14. Δεδομένα που αντλεί η εφαρμογή Netflix.

○ **Stremio**

Η πολιτική ιδιωτικότητας της εφαρμογής Stremio είναι σύντομη με αρκετές ελλείψεις. Οι ελλείψεις αυτές αφορούν τη συλλογή των δεδομένων αλλά και την παράλειψη αναφοράς των σκοπών χρήσης των προσωπικών δεδομένων των χρηστών. Συμπερασματικά, η εφαρμογή Stremio δεν θεωρείται πλήρης και κρίνεται ανεπαρκής αφού οι αδυναμίες της απειλούν την ιδιωτικότητα του χρήστη.

-Add Accounts -Remove Accounts	Πληροφορίες και Δημιουργία Λογαριασμού	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται από το χρήστη κατά τη δημιουργία λογαριασμού.
-Read Phone Status	Αναγνωριστικά Συσκευής, Διεύθυνση IP, Λειτουργικό Σύστημα	Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται αυτοματοποιημένα από την εφαρμογή.
- Receive Data Form Internet	Πληροφορίες μέσω τρίτων οντοτήτων για το χρήστη.	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα όταν ο χρήστης συνδεθεί μέσω τρίτης οντότητας (πχ Facebook, Google Play, iTunes).
-Network	Πλήρης πρόσβαση στο δίκτυο.	Δεν αναφέρεται στην πολιτική ιδιωτικότητας.

Πίνακας 15. Δεδομένα που αντλεί η εφαρμογή Stremio.

○ **Netflix & Stremio**

Συγκρίνοντας τις πολιτικές ιδιωτικότητας των δυο παρόμοιων εφαρμογών παρακολούθησης ταινιών και σειρών φαίνεται πως η πολιτική ιδιωτικότητας του Netflix παρουσιάζεται πολύ πιο ολοκληρωμένη, αφού η πολιτική του Stremio αποφεύγει να αναφέρει τις δυο πιο σημαντικές πτυχές μιας πολιτικής, τα δεδομένα που συλλέγει και το πως τα χρησιμοποιεί.

○ **Google Chrome**

Όπως αναφέρθηκε και στην ανάλυση της πολιτικής ιδιωτικότητας του Google Chrome, υπάρχουν τρεις επιλογές εισόδου διαθέσιμες για το χρήστη από τις οποίες εξαρτώνται και οι πληροφορίες που θα συλλέξει η εφαρμογή. Το Google Chrome συλλέγει πληροφορίες μόνο κατά την λειτουργία συγχρονισμού όπου ο χρήστης συνδέεται στον Google λογαριασμό του και επιλέγει το συγχρονισμό της συσκευής του. Ωστόσο, μελετώντας την άδεια απορρήτου της εφαρμογής παρατηρήθηκαν κάποιες ελλείψεις όσον αφορά ορισμένες επικίνδυνες άδειες στις οποίες έχει πρόσβαση η εφαρμογή χωρίς να αναφερθεί σε αυτές, στην πολιτική ιδιωτικότητας της. Οι επικίνδυνες αυτές άδειες αφορούν την πρόσβαση στις επαφές, στο μικρόφωνο και στον αποθηκευτικό χώρο.

Παράλληλα, ενώ αναλύονται διεξοδικώς οι τρόποι χρήσης των προσωπικών δεδομένων από την εφαρμογή, δεν γίνεται καμία αναφορά στους συνεργάτες και στις τρίτες οντότητες στις οποίες γνωστοποιεί τα δεδομένα των χρηστών η εφαρμογή.

Η αποφυγή της ενημέρωσης των χρηστών αναφορικά με τις επικίνδυνες άδειες, οι οποίες αποτελούν και το πιο σημαντικό κομμάτι μιας πολιτικής απορρήτου, σε συνδυασμό με την απουσία ενημέρωσης όσον αφορά τις πληροφορίες που γνωστοποιούνται σε τρίτες οντότητες, δημιουργούν ένα μεγάλο κενό στην ασφάλεια των χρηστών και η πολιτική ιδιωτικότητας του Google Chrome θεωρείται ελλιπής και αδιαφανής προς το χρήστη.

-Add Accounts -Remove Accounts -Find Accounts on Device -Toggle Sync On & Off -Read Sync Statistics -Read Sync Settings	Πληροφορίες και Δημιουργία Λογαριασμού, Διαδικασίες Συγχρονισμού	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται κατά τη δημιουργία λογαριασμού και επιλογής συγχρονισμού.
-Read History	Ιστορικό Αναζήτησης	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή. Στην επιλογή συγχρονισμού αποθηκεύεται στους Servers.
-Access Fine Location -Access Coarse Location	Τοποθεσία	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική

		ιδιωτικότητας/Αντλείται αν ο χρήστης το επιθυμεί. Αν ο χρήστης δώσει δικαίωμα τοποθεσίας στην εφαρμογή, αυτή μπορεί να δώσει την τοποθεσία του σε όλες τις ιστοσελίδες χωρίς την πληροφόρηση του.
-Read Contacts -Record Audio -Access Camera -Read Storage -Write Storage	Πρόσβαση σε : Επαφές, Κάμερα, Μικρόφωνο, Αποθηκευτικό Χώρο	Επικίνδυνες Άδειες. Δεν αναφέρονται στην πολιτική ιδιωτικότητας.

Πίνακας 16. Δεδομένα που αντλεί η εφαρμογή Google Chrome.

ο **Mozilla Firefox**

Ερευνώντας την πολιτική ιδιωτικότητας της εφαρμογής Mozilla Firefox, παρατηρήθηκε μεγάλη έλλειψη στον τομέα της συλλογής δεδομένων. Πιο συγκεκριμένα, στην πολιτική δεν γίνεται καμία αναφορά στα προσωπικά δεδομένα που η εφαρμογή συλλέγει από τους χρήστες της. Η πολιτική ιδιωτικότητας αφιερώνει το μεγαλύτερο μέρος της αναλύοντας το πως λαμβάνει τις πληροφορίες του χρήστη, δηλαδή μέσω των προϊόντων της και των συνεργατών της, καθώς και το πως χρησιμοποιεί τις πληροφορίες αυτές.

Η εφαρμογή Mozilla δεσμεύεται για την προστασία και ασφάλεια των δεδομένων και διατηρεί τα στοιχεία για όσο τα χρειάζεται και στη συνέχεια τα διαγράφει. Η δήλωση αυτή όμως δεν κρίνεται αρκετή για την ασφάλεια του χρήστη, καθώς η εφαρμογή αποφεύγοντας να γνωστοποιήσει τα προσωπικά δεδομένα που συλλέγει, δεν μπορεί να θεωρηθεί διαφανής και ξεκάθαρη ως προς τους χρήστες της.

-Add Accounts -Modify or remove Accounts -Find Accounts on Device -Toggle Sync On & Off -Read Sync Statistics -Read Sync Settings	Πληροφορίες και Δημιουργία Λογαριασμού, Διαδικασίες Συγχρονισμού	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας/Αντλούνται κατά τη δημιουργία λογαριασμού και επιλογής συγχρονισμού.
--	--	--

-Read History	Πληροφορίες Ιστορικού και Σελιδοδεικτών	Επικίνδυνες Άδειες. Δευ αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Access Fine Location -Access Coarse Location	Τοποθεσία	Επικίνδυνες Άδειες. Δευ αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Read Contacts -Record Audio -Access Camera -Read Storage -Write, Modify, Delete Storage	Πρόσβαση σε : Επαφές, Κάμερα, Μικρόφωνο, Πλήρης πρόσβαση στον Αποθηκευτικό Χώρο	Επικίνδυνες Άδειες. Δευ αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Internet -View Wi-Fi Connections -Full Network Access	Πληροφορίες Λειτουργικού Συστήματος, Διεύθυνση IP, Σημεία Πρόσβασης Διαδικτύου, Πλήρη πρόσβαση σε δίκτυο και Wi-Fi	Δευ αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Receive Data from Internet -Download Without Permission (Internet)	Πληροφορίες από Τρίτες Οντότητες, Λήψη αρχείων χωρίς ενημέρωση του χρήστη.	Επικίνδυνες Άδειες. Δευ αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.

Πίνακας 17. Δεδομένα που αντλεί η εφαρμογή Mozilla Firefox.

ο **Google Chrome & Mozilla Firefox**

Η αποφυγή της ενημέρωσης των χρηστών αναφορικά με τις επικίνδυνες άδειες, οι οποίες αποτελούν και το πιο σημαντικό κομμάτι μιας πολιτικής απορρήτου, σε συνδυασμό με την απουσία αναφοράς στην γνωστοποίηση δεδομένων σε τρίτες οντότητες, δημιουργούν ένα μεγάλο κενό στην ασφάλεια των χρηστών και η πολιτική ιδιωτικότητας του Google Chrome θεωρείται ελλιπής και αδιαφανής προς το χρήστη.

Από την άλλη μεριά, η πολιτική ιδιωτικότητας του Mozilla Firefox κρίνεται επίσης ανεπαρκής, λόγω της μεγάλης έλλειψης στον τομέα της συλλογής δεδομένων. Καμία από τις δυο εφαρμογές δεν θεωρείται διαφανής προς το χρήστη.

ο **Skype**

Η πολιτική ιδιωτικότητας του Skype αφιερώνει το μεγαλύτερο κομμάτι της στους σκοπούς και τρόπους χρήσης των δεδομένων. Κάτι τέτοιο όμως δεν θεωρείται αρκετό καθώς δεν κάνει καμία αναφορά στα προσωπικά δεδομένα των χρηστών που συλλέγει, τα οποία αποτελούν και το πιο σημαντικό κομμάτι μιας πολιτικής απορρήτου.

Συνοψίζοντας, η πολιτική ιδιωτικότητας του Skype δεν θεωρείται επαρκής καθώς δεν κάνει καμία αναφορά στα προσωπικά δεδομένα των χρηστών τα οποία συλλέγει.

-Internet -View Wi-Fi Connections -Full Network Access -Access Bluetooth Settings	Σημεία Πρόσβασης Διαδικτύου, Πλήρη πρόσβαση σε δίκτυο ,Wi-Fi και Bluetooth.	Δεν αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Access Fine Location -Access Coarse Location	Τοποθεσία	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Read Contacts -Record Audio -Access Camera -Read Storage -Write, Modify, Delete Storage, -Read /Write Calendar	Πρόσβαση σε : Επαφές, Κάμερα, Μικρόφωνο, Πλήρης πρόσβαση στον Αποθηκευτικό Χώρο, Ημερολόγιο.	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Add Accounts -Modify or remove Accounts -Find Accounts on Device -Toggle Sync On & Off -Read Sync Statistics -Read Sync Settings	Πληροφορίες και Δημιουργία Λογαριασμού, Διαδικασίες Συγχρονισμού	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλούνται κατά τη δημιουργία λογαριασμού και επιλογής συγχρονισμού.

-Read Phone Status	Κατάσταση Συσκευής	Δεν αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Receive Data from Internet -Download Files Without Permission (Internet)	Πληροφορίες από Τρίτες Οντότητες, Λήψη αρχείων χωρίς ενημέρωση του χρήστη.	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.

Πίνακας 18. Δεδομένα που αντλεί η εφαρμογή Skype.

ο **Zoom**

Η πολιτική ιδιωτικότητας της εφαρμογής Zoom εμφανίζεται ιδιαίτερα κατατοπιστική ως προς τα προσωπικά δεδομένα που συλλέγει αλλά και τον τρόπο χρήσης τους. Επιπλέον, η εφαρμογή απαριθμεί κάποιους τρόπους άντλησης των δεδομένων, όμως δεν αναφέρεται σχολαστικά στους συνεργάτες και στις τρίτες οντότητες με τις οποίες διαμοιράζεται τα προσωπικά στοιχεία.

Συνοψίζοντας, η πολιτική ιδιωτικότητας της εφαρμογής Zoom κρίθηκε αρκετά σαφής προς το χρήστη και τα δεδομένα του, με κάποιες ελλείψεις στον τομέα των τρίτων οντοτήτων.

-Add Accounts -Remove Accounts	Πληροφορίες και Δημιουργία Λογαριασμού	Επικίνδυνες Άδειες. Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται κατά τη δημιουργία λογαριασμού.
-Modify System Settings -Read Phone Status	Αναγνωριστικά Συσκευής, Διεύθυνση IP, Λειτουργικό Σύστημα	Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Internet -View Wi-Fi Connections	Σημεία Πρόσβασης Διαδικτύου, Πλήρη πρόσβαση σε	Αναφέρεται στην πολιτική ιδιωτικότητας/ Αντλείται

-Full Network Access -Access Bluetooth Settings	δίκτυο ,Wi-Fi και Bluetooth. Πληροφορίες Λειτουργικού Συστήματος, Διεύθυνση IP,	αυτοματοποιημένα από την εφαρμογή.
-Read Contacts -Record Audio -Access Camera -Read Storage -Write, Modify, Delete Storage, -Read/Write Calendar	Πρόσβαση σε : Επαφές, Κάμερα, Μικρόφωνο, Πλήρης πρόσβαση στον Αποθηκευτικό Χώρο, Ημερολόγιο.	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας/Αντλείται αυτοματοποιημένα από την εφαρμογή.
-Receive Data from Internet	Πληροφορίες από Τρίτες Οντότητες	Επικίνδυνες Άδειες. Δεν αναφέρεται στην πολιτική ιδιωτικότητας/Αντλείται αυτοματοποιημένα από την εφαρμογή.

Πίνακας 19. Δεδομένα που αντλεί η εφαρμογή Zoom.

ο **Skype & Zoom**

Μελετώντας τις πολιτικές ιδιωτικότητας των δυο πιο επιτυχημένων εφαρμογών τηλεδιάσκεψης παρατηρήθηκε μεγάλη διαφορά στη προσέγγιση τους. Το Skype δεν αναφέρεται καθόλου στα προσωπικά δεδομένα που συλλέγει ενώ το Zoom εμφανίζεται πλήρως επεξηγηματικό. Ωστόσο, το πρώτο αφιερώνει το μεγαλύτερο μέρος της πολιτικής απορρήτου του, απαριθμώντας τις πηγές από τις οποίες αντλεί τα δεδομένα των χρηστών, ενώ το Zoom αποφεύγει τον καθορισμό των συνεργατών του. Όσον αφορά τους τρόπους με τους οποίους χειρίζονται τα δεδομένα, φαίνονται το ίδιο επεξηγηματικοί και πλήρεις.

Έπειτα από μελέτη, συμπεραίνεται ότι η πολιτική ιδιωτικότητας του Zoom παρουσιάζεται πιο ολοκληρωμένη σε σχέση με αυτή του Skype, λόγω του ότι αναλύει διεξοδικώς ποια δεδομένα των χρηστών συλλέγει, αντικείμενο μεγίστης σημασίας για την ασφάλεια του χρήστη.

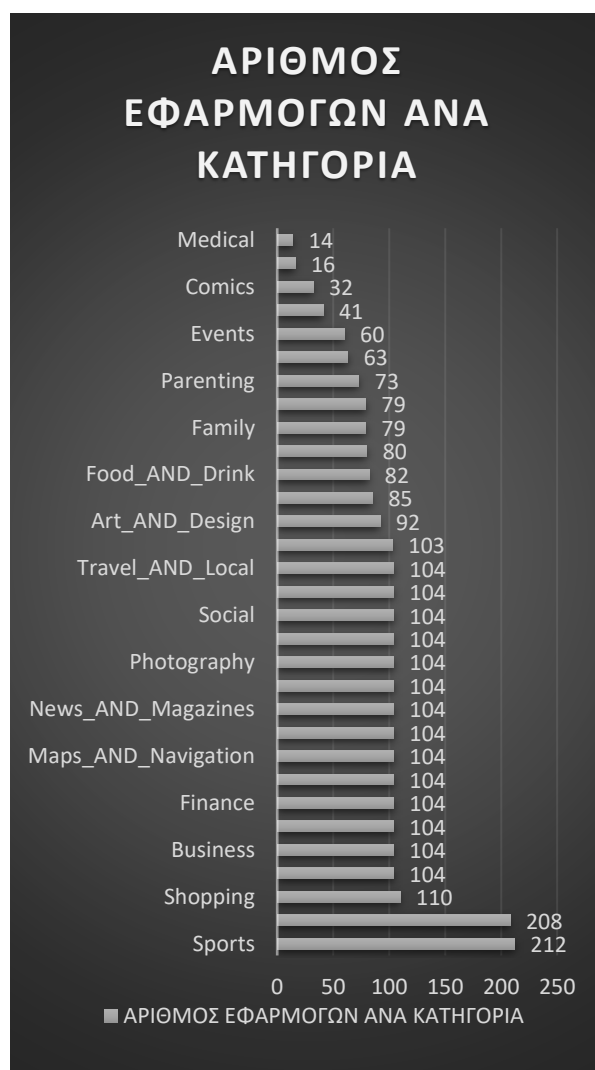
Το γενικότερο συμπέρασμα που δημιουργήθηκε μετά τη μελέτη και την ανάλυση των δέκα πολιτικών ιδιωτικότητας είναι όλες οι πολιτικές διαθέτουν τουλάχιστον μια έλλειψη σε κάποια από τις πέντε πτυχές τους. Ωστόσο, οι πολιτικές ιδιωτικότητας που φαίνεται να είναι πιο ξεκάθαρες και ειλικρινείς απέναντι στο χρήστη είναι αυτές του

Facebook, WhatsApp και Netflix και αυτές που κρίθηκαν πιο αδύναμες και ελλιπείς, φαίνεται να είναι αυτές των εφαρμογών Mozilla Firefox και Google Chrome.

4.5 Αποτελέσματα από την Εκτέλεση των SQL Ερωτημάτων

Τα αποτελέσματα που παρουσιάζονται σε αυτό το κεφάλαιο έχουν σχηματισθεί μετά την εκτέλεση του κώδικα για την άντληση των δεδομένων από το Google Play και έπειτα την εκτέλεση SQL ερωτημάτων ή queries.

❖ Ο ΑΡΙΘΜΟΣ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΠΟΥ ΜΕΛΕΤΗΘΗΚΑΝ ΑΝΑ ΚΑΤΗΓΟΡΙΑ ΤΟΥ GOOGLE PLAY



Πίνακας 20. Αριθμός εφαρμογών που μελετήθηκαν ανά κατηγορία του Google Play.

❖ **ΕΡΩΤΗΜΑ 1 : ΠΛΗΘΟΣ ΑΔΕΙΩΝ ΠΡΟΣΒΑΣΗΣ ΑΝΑ ΕΦΑΡΜΟΓΗ**

QUERY :

```
SELECT B.DESCR APP,COUNT(A.APPS) PERMISSIONS
FROM APPSPERMISSIONSDetail A
JOIN APPS B ON B.PK=A.APPS
GROUP BY B.DESCR
ORDER BY 2 DESC
```

ΑΠΟΤΕΛΕΣΜΑΤΑ :

Από το ερώτημα αυτό, πληροφορούμαστε πως από τις 3026 εφαρμογές που μελετούμε συνολικά, οι 2749 ζητούν έστω και μια άδεια πρόσβασης από το χρήστη, ενώ 277 εφαρμογές δεν ζητούν καμία άδεια. Πρώτη βρίσκεται η “Weather Forecast” η οποία ζητά 107 άδειες ενώ τελευταία βρίσκεται η “Vehicle Plate Codes of Russia” η οποία ζητά 1 και μόνο άδεια.

(Δείγμα των αποτελεσμάτων από τα πλήθη αδειών πρόσβασης των 3026 εφαρμογών.)

A/A	ΕΦΑΡΜΟΓΕΣ	ΑΔΕΙΕΣ
1	Weather Forecast	107
2	Music Player	97
3	Parallel Space	95
4	Music player	76
5	HelloTalk	70
6	Amazfit	66
7	Samsung Email	63
8	Coursera: Online Courses	61
9	All Football	58
10	Globoesporte.com	58
11	Snap Homework App	58
12	Uolo Notes	56
13	Microsoft Launcher	55
14	Live Score	54
15	MIT AI2 Companion	54
16	Poco Launcher 2.0	54
17	Samsung Smart Switch Mobile	53
18	Wella-Audio Book	52
19	Weather	51
20	FC Koln App	50

21	<i>Classting: Class Communication</i>	50
22	<i>Free phone calls, free texting SMS on free number</i>	50
23	<i>MyClassBoard Parent Portal</i>	50
24	<i>QQ</i>	50
25	<i>SHAREit – Transfer & Share</i>	50
26	<i>Mi Home</i>	49
27	<i>TrueCaller</i>	49
28	<i>CallApp: Caller ID, Call Blocker & Call Recorder</i>	48
29	<i>FC Barcelona Official App</i>	48
30	<i>Next Learning Platform</i>	48

Πίνακας 21. Πλήθος αδειών πρόσβασης ανά εφαρμογή(Δείγμα)

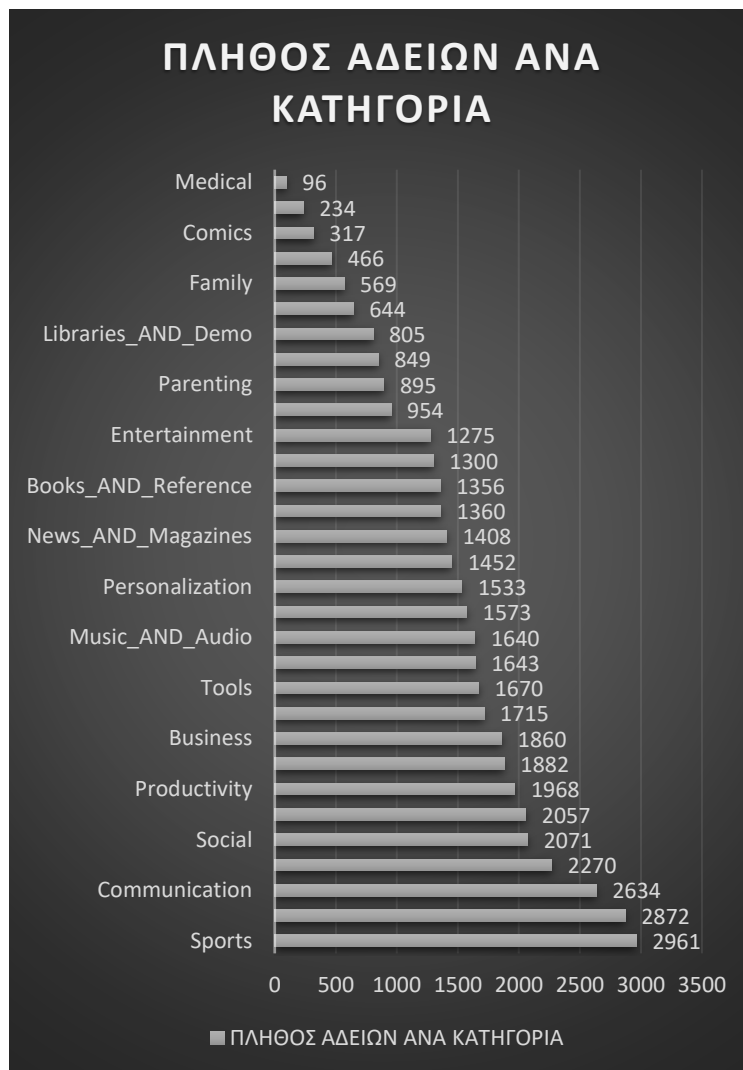
❖ ΕΡΩΤΗΜΑ 2 : ΠΛΗΘΟΣ ΑΔΕΙΩΝ ΑΝΑ ΚΑΤΗΓΟΡΙΑ

QUERY :

```
SELECT C.DESCR,COUNT(D.APPS)
FROM CATEGORIES C
LEFT OUTER JOIN APPS B ON C.PK=B.CATEGORIES
LEFT OUTER JOIN APPSPERMISSIONSDetail D ON
D.APPS=B.PK
GROUP BY C.DESCR
```

ΑΠΟΤΕΛΕΣΜΑΤΑ :

Παρατηρούμε ότι οι εφαρμογές που προέρχονται από την κατηγορία “sports”, ζητούν τα περισσότερα δικαιώματα από όλες τις εφαρμογές των υπόλοιπων κατηγοριών. Αυτό μπορεί να συμβαίνει είτε λόγω του ότι η κατηγορία sports περιέχει εφαρμογές όπου οι χρήστες στοιχηματίζουν σε αγώνες και έτσι παρέχουν πρόσβαση σε πολλές επικίνδυνες άδειες όπως πληρωμές, κάρτες κ.α. είτε γιατί οι δημιουργοί των εφαρμογών της κατηγορίας αυτής, ζητούν ανεξέλεγκτα πρόσβαση σε πολλές άδειες από το χρήστη. Από την άλλη μεριά, η κατηγορία με τις εφαρμογές που ζητούν τις λιγότερες άδειες εμφανίζεται να είναι η κατηγορία “medical”.



Πίνακας 22. Πλήθος αδειών ανά κατηγορία.

❖ **ΕΡΩΤΗΜΑ 3 : ΟΙ 40 ΕΦΑΡΜΟΓΕΣ ΠΟΥ ΖΗΤΟΥΝ ΤΑ ΠΕΡΙΣΣΟΤΕΡΑ ΔΙΚΑΙΩΜΑΤΑ**

QUERY:

```
SELECT B.DESCR APP, COUNT(A.APPS) PERMISSIONS
FROM APPSPERMISSIONSDetail A
JOIN APPS B ON B.PK=A.APPS
GROUP BY B.DESCR
ORDER BY 2 DESC
LIMIT 40;
```

ΑΠΟΤΕΛΕΣΜΑΤΑ:

Η εφαρμογή που ζητά τα περισσότερα δικαιώματα εμφανίζεται να είναι η "Weather Forecast" με 107 άδειες, γεγονός αξιοσημείωτο

καθώς μια εφαρμογή που έχει ως στόχο να ενημερώσει το χρήστη για τα καιρικά φαινόμενα, θα περιμέναμε να ζητά λίγες και συγκεκριμένες άδειες πρόσβασης όπως τοποθεσία και πρόσβαση στο Internet. Παράλληλα, παρατηρούμε πως στις πρώτες 50 εφαρμογές οι οποίες ζητούν τα περισσότερα δικαιώματα, εμπεριέχονται κάποιες πολύ διαδεδομένες εφαρμογές όπως η Facebook, Messenger, Microsoft, Samsung Email, UC Browser κ.α.

A/A	ΕΦΑΡΜΟΓΕΣ	ΑΔΕΙΕΣ
1	<i>Weather Forecast</i>	107
2	<i>Music Player</i>	97
3	<i>Parallel Space</i>	95
4	<i>Music player</i>	76
5	<i>HelloTalk</i>	70
6	<i>Amazfit</i>	66
7	<i>Samsung Email</i>	63
8	<i>Coursera: Online Courses</i>	61
9	<i>All Football</i>	58
10	<i>Globoesporte.com</i>	58
11	<i>Snap Homework App</i>	58
12	<i>Uolo Notes</i>	56
13	<i>Microsoft Launcher</i>	55
14	<i>Live Score</i>	54
15	<i>MIT AI2 Companion</i>	54
16	<i>Poco Launcher 2.0</i>	54
17	<i>Samsung Smart Switch Mobile</i>	53
18	<i>Wella-Audio Book</i>	52
19	<i>Weather</i>	51
20	<i>FC Koln App</i>	50
21	<i>Classting: Class Communication</i>	50
22	<i>Free phone calls, free texting SMS on free number</i>	50
23	<i>MyClassBoard Parent Portal</i>	50
24	<i>QQ</i>	50
25	<i>SHAREit – Transfer & Share</i>	50
26	<i>Mi Home</i>	49
27	<i>TrueCaller</i>	49
28	<i>CallApp: Caller ID, Call Blocker & Call Recorder</i>	48
29	<i>FC Barcelona Official App</i>	48
30	<i>Next Learning Platform</i>	48
31	<i>Ruangguru - One-stop Learning Solution</i>	48
32	<i>Samsung Internet Browser</i>	48

33	<i>МАТЧ! – смотреть спорт онлайн</i>	48
34	<i>Huawei Health</i>	47
35	<i>Aakash iTutor Learning App</i>	46
36	<i>Exam Prep : Free Videos, Live Classes & Mock Tests</i>	46
37	<i>Golf GPS & Scorecard by SwingU</i>	46
38	<i>Messenger – Text and Video Chat for Free</i>	46
39	<i>U-Dictionary: Oxford Dictionary Free Now Translate</i>	46
40	<i>UC Browser- Free & Fast Video Downloader, News App</i>	46

Πίνακας 23. Οι 40 εφαρμογές που ζητούν τα περισσότερα δικαιώματα.

❖ **ΕΡΩΤΗΜΑ 4 : ΟΙ 30 ΕΦΑΡΜΟΓΕΣ ΠΟΥ ΖΗΤΟΥΝ ΤΑ ΛΙΓΟΤΕΡΑ ΔΙΚΑΙΩΜΑΤΑ**

QUERY:

```
SELECT A.APPS,B.DESCR,COUNT(A.APPSPERMISSIONS)
plithos
FROM APPSPERMISSIONSDetail A
JOIN APPS B on B.PK=A.APPS
GROUP BY A.APPS,B.DESCR
ORDER by 3 ASC
LIMIT 30;
```

ΑΠΟΤΕΛΕΣΜΑΤΑ:

Αυτές είναι οι 30 εφαρμογές που ζητούν τα λιγότερα δικαιώματα.

A/A	ΕΦΑΡΜΟΓΕΣ	ΑΔΕΙΕΣ
1	<i>Vehicle Plate Codes of Russia</i>	1
2	<i>Diccionario RAE y ASALE (DLE)</i>	1
3	<i>Socrative Student</i>	1
4	<i>Germany Holiday Calendar</i>	1
5	<i>Ayush Sanjivani</i>	1
6	<i>Pitch Black Wallpaper</i>	1
7	<i>CPU-Z</i>	1

8	Boju weather icons	1
9	3D Love Stickers For WhatsApp 2020	2
10	WASStickerApps Couple Love Romance Sticker	2
11	Flying Robot Car War Transform Fight	2
12	Golden Dictionary (EN-AR)	2
13	Personal stickers for WhatsApp	2
14	Animal sounds for kids	2
15	My Reminders	2
16	SuperCook: Recipes By Ingredient	2
17	Ministro II	2
18	Wi-Fi Connector Library	2
19	Monash Uni Low FODMAP Diet	2
20	All Bangla Newspapers	2
21	Ad-Free Baby Night Light	2
22	Color Changer Free [root]	2
23	All Network Packages 2020	2
24	Sports Predictions	2
25	Coloring Games: Coloring Book, Painting, Glow Draw	2
26	Logic Puzzles - Brain Fun	2
27	Wallpaper WINX Club	3
28	How to make doll clothes	3
29	Spanish English Translator	3
30	Best Cat Stickers for Chat WASStickerApps	3

Πίνακας 24. Οι 30 εφαρμογές που ζητούν τα λιγότερα δικαιώματα.

❖ **ΕΡΩΤΗΜΑ 5 : ΟΙ 30 ΕΦΑΡΜΟΓΕΣ ΠΟΥ ΖΗΤΟΥΝ ΤΙΣ ΠΕΡΙΣΣΟΤΕΡΕΣ ΕΠΙΚΙΝΔΥΝΕΣ ΑΔΕΙΕΣ**

QUERY :

```
SELECT* FROM
(SELECT DISTINCT C.DESCR,COUNT(A.CRUSIAL)
FROM APPSPERMISSIONS A
JOIN APPSPERMISSIONSDetail b on
b.APPSPERMISSIONS=a.pk
JOIN APPS C on C.PK=B.APPS
```

WHERE A.CRUSIAL = 'true'
 GROUP BY C.DESCR
) Z
 ORDER BY 2 DESC;
 LIMIT 30;

ΑΠΟΤΕΛΕΣΜΑΤΑ:

A/A	ΕΦΑΡΜΟΓΕΣ	ΠΛΗΘΟΣ
1	POCO Launcher 2.0 - Customize, Fresh & Clean	52
2	Truecaller	45
3	UC Browser	45
4	Championat	42
5	U-Dictionary: Oxford Dictionary	42
6	SmartThings	41
7	Maps - Navigate & Explore	37
8	Parallel Space Lite	37
9	Music Player	35
10	Amazfit	32
11	Arlo	31
12	IP Pro (VR Cam, Selwood)	31
13	LG ThinQ	31
14	Weather Forecast	31
15	MIT AI2 Companion	30
16	Samsung Notes	30
17	Snap Homework App	30
18	AirAsia	28
19	Coursera: Online courses	28
20	4shared	27
21	Music player	27
22	Aakash iTutor Learning App	26
23	Doubtnut	26
24	FC Barcelona Official App	26
25	HelloTalk	26
26	Minha Oi - Conta	26
27	Team App	26
28	Microsoft Launcher	25
29	삼성카드	25
30	All Football	24

Πίνακας 25. Οι 30 εφαρμογές που ζητούν τις περισσότερες επικίνδυνες άδειες.

❖ **ΕΡΩΤΗΜΑ 6: ΟΙ 30 ΑΔΕΙΕΣ ΠΟΥ ΖΗΤΟΥΝΤΑΙ ΠΕΡΙΣΣΟΤΕΡΟ ΑΠΟ ΤΙΣ ΕΦΑΡΜΟΓΕΣ**

QUERY:

```
SELECT A.DESCR, count(A.DESCR)
FROM APPSPERMISSIONSDetail A
GROUP BY A.DESCR
ORDER BY 2 DESC;
```

ΑΠΟΤΕΛΕΣΜΑΤΑ:

Βλέποντας τον παρακάτω πίνακα παρατηρούμε ότι το πλήθος των δυο πρώτων δικαιωμάτων είναι μεγαλύτερο από το σύνολο των εφαρμογών. Αυτό συμβαίνει γιατί ορισμένες εφαρμογές αναφέρουν κάποιες άδειες δυο φορές. Παράλληλα, διακρίνουμε ότι από τις 30 πιο πολύ ζητημένες άδειες, οι περισσότερες ανήκουν στις επικίνδυνες άδειες καθώς αναφέρονται σε τοποθεσία, ήχο, εικόνα, βίντεο, αποθηκευτικό χώρο ή επαφές.

A/A	ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ	ΠΛΗΘΟΣ
1	Read the contents of your USB storage	5004
2	Modify or delete the contents of your USB storage	4859
3	Full network access	2981
4	View network connections	2963
5	Prevent device from sleeping	2835
6	Receive data from Internet	2563
7	Read phone status and identity	2162
8	View Wi-Fi connections	1935
9	Control vibration	1789
10	Find accounts on the device	1682
11	Run at startup	1679
12	Precise location (GPS and network-based)	1487
13	Take pictures and videos	1353
14	Approximate location (network-based)	1324
15	Record audio	716
16	Read Google service configuration	693
17	Read your contacts	623
18	Pair with Bluetooth devices	612
19	Draw over other apps	587

20	Connect and disconnect from Wi-Fi	530
21	Change your audio settings	429
22	Use accounts on the device	408
23	Retrieve running apps	399
24	Access Bluetooth settings	356
25	Directly call phone numbers	337
26	Add or remove accounts	314
27	Install shortcuts	308
28	Create accounts and set passwords	300
29	Modify system settings	298
30	Change network connectivity	275

Πίνακας 26. Οι 30 άδειες που ζητούνται περισσότερο από τις εφαρμογές.

❖ **ΑΝΤΙΣΤΟΙΧΙΣΗ ΤΩΝ 30 ΑΔΕΙΩΝ ΜΕ ΤΙΣ ΑΔΕΙΕΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ANDROID**

A/A	ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ	ΟΝΟΜΑ ΑΔΕΙΑΣ ΛΕΙΤΟΥΡΓΙΚΟΥ
1	Read the contents of your USB storage	READ_EXTERNAL_STORAGE
2	Modify or delete the contents of your USB storage	WRITE_EXTERNAL_STORAGE
3	Full network access	ACCESS_NETWORK_STATE CHANGE_NETWORK_STATE
4	View network connections	ACCESS_NETWORK_STATE
5	Prevent device from sleeping	WAKE_LOCK
6	Receive data from Internet	INTERNET
7	Read phone status and identity	READ_PHONE_STATE
8	View Wi-Fi connections	ACCESS_WIFI_STATE
9	Control vibration	VIBRATE
10	Find accounts on the device	GET_ACCOUNTS
11	Run at startup	RECEIVE_BOOT_COMPLETED
12	Precise location (GPS and network-based)	ACCESS_FINE_LOCATION
13	Take pictures and videos	CAMERA
14	Approximate location (network-based)	ACCESS_COARSE_LOCATION
15	Record audio	RECORD_AUDIO
16	Read Google service configuration	Google does not explicitly provide documentation for this permission.

17	Read your contacts	READ_CONTACTS
18	Pair with Bluetooth devices	BLUETOOTH
19	Draw over other apps	SYSTEM_ALERT_WINDOW
20	Connect and disconnect from Wi-Fi	CHANGE_WIFI_STATE
21	Change your audio settings	MODIFY_AUDIO_SETTINGS
22	Use accounts on the device	MANAGE_ACCOUNTS
23	Retrieve running apps	GET_TASKS
24	Access Bluetooth settings	BLUETOOTH_ADMIN
25	Directly call phone numbers	WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS
26	Add or remove accounts	MANAGE_ACCOUNTS
27	Install shortcuts	INSTALL_SHORTCUT
28	Create accounts and set passwords	ACCOUNT_MANAGER, MANAGE_ACCOUNTS
29	Modify system settings	WRITE_SECURE_SETTINGS
30	Change network connectivity	CHANGE_NETWORK_STATE

Πίνακας 27. Αντιστοίχιση των 30 αδειών με τις άδειες του λειτουργικού συστήματος Android.

❖ **ΕΡΩΤΗΜΑ 7: ΟΙ 30 ΑΔΕΙΕΣ ΠΟΥ ΖΗΤΟΥΝΤΑΙ ΛΙΓΟΤΕΡΟ ΑΠΟ ΤΙΣ ΕΦΑΡΜΟΓΕΣ**

QUERY:

```
SELECT A.DESCR, count(A.DESCR)
FROM APPSPERMISSIONSDETAIL A
GROUP BY A.DESCR
ORDER BY 2 ASC;
```

ΑΠΟΤΕΛΕΣΜΑΤΑ:

A/A	ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ	ΠΛΗΘΟΣ
1	Access Surface Flinger	1
2	Access content providers externally	1
3	Access the cache filesystem	1
4	Add or remove a device admin	1
5	Bind to a VPN service	1
6	Bind to a print service	1
7	Bind to a widget service	1
8	Change screen orientation	1
9	Connect and disconnect from WiMAX	1
10	Control location update notifications	1

11	Control system backup and restore	1
12	Delete other apps' caches	1
13	Erase USB storage	1
14	Interact with a device admin	1
15	Invoke the carrier-provided configuration app	1
16	Manage app tokens	1
17	Manage network policy	1
18	Manage preferences and permissions for USB devices	1
19	Read instant messages	1
20	Read precise phone states	1
21	Read voicemail	1
22	Reset system to factory defaults	1
23	Send SMS-received broadcast	1
24	Send WAP-PUSH-received broadcast	1
25	Start a task from recents	1
26	Stop running apps	1
27	Use any media decoder for playback	1
28	Write instant messages	1
29	Write voicemails	1
30	Add voicemail	2

Πίνακας 28. Οι 30 άδειες που ζητούνται λιγότερο από τις εφαρμογές.

❖ **ΕΡΩΤΗΜΑ 8: ΟΙ 30 ΑΔΕΙΕΣ ΠΟΥ ΖΗΤΟΥΝΤΑΙ ΠΕΡΙΣΣΟΤΕΡΟ ΚΑΙ ΤΟ ΠΟΣΟΣΤΟ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΠΟΥ ΤΙΣ ΖΗΤΟΥΝ**

QUERY:

```
SELECT A.DESCR, COUNT(APPS), ROUND(
CAST(COUNT(APPS)AS REAL)/(SELECT COUNT(PK) FROM
APPS) * 100 ,2) PERCENTOFPERRMISSIONSINAPPS
FROM APPSPERMISSIONSDETAIL A
GROUP BY A.DESCR
ORDER BY 2 DESC;
```

ΑΠΟΤΕΛΕΣΜΑΤΑ:

A/A	ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ	ΠΟΣΟΣΤΟ ΕΜΦΑΝΙΣΗΣ
1	Read the contents of your USB storage	100%
2	Modify or delete the contents of your USB storage	100%
3	Full network access	98.51%
4	View network connections	97.92%
5	Prevent device from sleeping	93.69%
6	Receive data from Internet	84.7%
7	Read phone status and identity	71.45%
8	View Wi-Fi connections	63.95%
9	Control vibration	59.12%
10	Find accounts on the device	55.58%
11	Run at startup	55.49%
12	Precise location (GPS and network-based)	49.14%
13	Take pictures and videos	44.71%
14	Approximate location (network-based)	43.75%
15	Record audio	23.66%
16	Read Google service configuration	22.9%
17	Read your contacts	20.59%
18	Pair with Bluetooth devices	20.22%
19	Draw over other apps	19.4%
20	Connect and disconnect from Wi-Fi	17.51%
21	Change your audio settings	14.18%
22	Use accounts on the device	13.48%
23	Retrieve running apps	13.19%
24	Access Bluetooth settings	11.76%
25	Directly call phone numbers	11.14%
26	Add or remove accounts	10.38%
27	Install shortcuts	10.18%
28	Create accounts and set passwords	9.91%
29	Modify system settings	9.85%
30	Change network connectivity	9.09%

Πίνακας 29. Οι 30 άδειες που ζητούνται περισσότερο και το ποσοστό των εφαρμογών που τις ζητούν.

❖ **ΕΡΩΤΗΜΑ 9: ΟΙ ΕΠΙΚΙΝΔΥΝΕΣ ΑΔΕΙΕΣ ΚΑΙ ΤΟ ΠΟΣΟΣΤΟ ΕΦΑΡΜΟΓΩΝ ΠΟΥ ΤΙΣ ΖΗΤΟΥΝ**

QUERY:

```
SELECT A.DESCR, COUNT(APPS), ROUND(
CAST(COUNT(APPS)AS REAL)/ (SELECT COUNT(PK) FROM
APPS) * 100 ,2) PERCENTOFPERRMISSIONSINAPPS
,B.DESCR,B.CRUSIAL
FROM APPSPERMISSIONSDetail A
JOIN APPSPERMISSIONS B ON A.APPSPERMISSIONS=B.PK
WHERE B.CRUSIAL ='true'
GROUP BY A.DESCR
ORDER BY 2 DESC
```

ΑΠΟΤΕΛΕΣΜΑΤΑ:

A/A	ΕΠΙΚΙΝΔΥΝΕΣ ΑΔΕΙΕΣ ΠΡΟΣΒΑΣΗΣ	ΠΟΣΟΣΤΟ ΕΜΦΑΝΙΣΗΣ
1	READ_EXTERNAL_STORAGE	100%
2	WRITE_EXTERNAL_STORAGE	100%
3	INTERNET	84,7%
4	READ_PHONE_STATE	71,45%
5	GET_ACCOUNTS	55,58%
6	ACCESS_FINE_LOCATION	49.14%
7	CAMERA	44.71%
8	ACCESS_COARSE_LOCATION	43.75%
9	ACCESS_NETWORK_STATE	32,40%
10	RECORD_AUDIO	23.66%
11	GET_TASKS	12.95%
12	CALL_PHONE	11.14%
13	WRITE_CONTACTS	10.38%
14	READ_CALENDAR	4.90%
15	WRITE_CALENDAR	4.23%
16	READ_PROFILE	3.47%
17	READ_LOGS	3.21%
18	RECEIVE_SMS	1.35%
19	READ_SMS	1.26%
20	SEND_SMS	0.79%
21	READ_CALL_LOG	0,78%
22	WRITE_CALL_LOG	0,77%
23	PROCESS_OUTGOING_CALLS	0,69%
24	ANSWER_PHONE_CALLS	0,59%
25	BODY_SENSORS	0,43 %
26	RECEIVE_MMS	0,50%

27	READ_PHONE_NUMBERS	0,38%
28	USE_SIP	0,23%
29	ADD_VOICEMAIL	0,07%
30	WRITE_VOICEMAIL	0,03%

Πίνακας 30. Οι επικίνδυνες άδειες και το ποσοστό εφαρμογών που τις ζητούν.

5. Συμπεράσματα

Η παρούσα πτυχιακή είχε ως αντικείμενο της, δυο διαφορετικές πτυχές της ιδιωτικότητας των χρηστών των εφαρμογών Android. Το πρώτο μέρος αφορούσε την ανάλυση και μελέτη των αδειών πρόσβασης, που ζητούν από τους χρήστες, εκατοντάδες εφαρμογές του Google Play και το δεύτερο μέρος σχετιζόταν με την έρευνα και ανάλυση των πολιτικών ιδιωτικότητας δέκα δημοφιλών εφαρμογών του Google Play. Μεγάλη ανησυχία δημιουργήθηκε κατά τη συγγραφή της πτυχιακής, από την έλλειψη επαρκούς προστασίας των προσωπικών δεδομένων των χρηστών που παρατηρήθηκε από ένα λειτουργικό σύστημα τόσο διαδεδομένο, σαν το Android.

Μετά από μεγάλη μελέτη, η οποία παρουσιάστηκε στα προηγούμενα κεφάλαια, καταλήξαμε στα εξής συμπεράσματα:

- ❖ Λόγω του ότι το Google Play αποτελεί ένα δημοφιλές και φαινομενικά αξιόπιστο site, αναμέναμε μεγαλύτερη διαφύλαξη της ιδιωτικότητας του χρήστη. Από τα αποτελέσματα μας παρατηρήθηκε όμως, ότι πάρα πολλές και γνωστές εφαρμογές του Play Store ζητούν επικίνδυνα δικαιώματα χωρίς να είναι αναγκαία για τη λειτουργικότητα τους. Σε αυτό το συμπέρασμα προβαίνουμε αν παρατηρήσουμε τους **Πίνακα 21** και **Πίνακα 23** όπου για παράδειγμα η εφαρμογή που ζητά τις πιο πολλές άδειες και τις πιο επικίνδυνες ταυτόχρονα, ονομάζεται “Weather Forecast”, η οποία σκοπό έχει την ενημέρωση του χρήστη για τον καιρό. Για την επίτευξη της λειτουργίας αυτής είναι προφανές ότι δεν είναι αναγκαία η πρόσβαση της εφαρμογής στα προσωπικά δεδομένα του χρήστη, εκτός από την τοποθεσία, και η εφαρμογή κακώς ζητά αλόγιστη πρόσβαση στα δεδομένα του χρήστη.
- ❖ Παράλληλα, από τον **Πίνακα 23**, παρατηρούμε ότι στις 40 εφαρμογές που ζητούν τις περισσότερες άδειες από τους χρήστες, συμπεριλαμβάνονται πολύ γνωστές εφαρμογές όπως Facebook, Messenger, Microsoft, Samsung Email, UC Browser, εφαρμογές με δισεκατομμύρια χρήστες ημερησίως. Τα αποτελέσματα αυτά, θεωρούνται ικανά για να αφυπνίσουν τους χρήστες ως προς τις εφαρμογές που επιλέγουν να εγκαταστήσουν.

- ❖ Συμπεραίνουμε επίσης, ότι η κατηγορία του Google Play που περιέχει τις εφαρμογές που ζητούν τις περισσότερες άδειες φαίνεται να είναι η κατηγορία “Sports”.
- ❖ Καταλήξαμε επίσης στο γεγονός ότι, ο μεγαλύτερος εχθρός του χρήστη φαίνεται να είναι το ίδιο το λειτουργικό σύστημα Android, καθώς μπορεί να έχει πρόσβαση σε όλα τα προσωπικά δεδομένα του χρήστη.
- ❖ Μελετώντας τον **Πίνακα 24**, παρατηρούμε ότι οι εφαρμογές που ζητούν τις λιγότερες άδειες, εξυπηρετούν μια και μοναδική λειτουργία και ανάγκη του χρήστη, για παράδειγμα “Wallpapers”. Πολλές από αυτές επίσης, αφορούν μικρότερες ηλικίες και παιδιά.
- ❖ Μελετώντας τον **Πίνακα 29**, συμπεραίνουμε ότι τα ποσοστά ζήτησης των επικίνδυνων αδειών από τις εφαρμογές είναι τεράστια, και μάλιστα μερικά ποσοστά αγγίζουν το 90-100%. Επικίνδυνες άδειες όπως πρόσβαση στον αποθηκευτικό χώρο, στην κάμερα, στις επαφές του χρήστη και στην τοποθεσία του, φαίνεται να ζητούνται από τις περισσότερες εφαρμογές του δείγματος μας, γεγονός που θα πρέπει να αφυπνίζει και να ανησυχεί τους χρήστες.
- ❖ Στο δεύτερο μέρος της πτυχιακής, ερευνώντας τις πολιτικές ιδιωτικότητας των εφαρμογών, καταλήξαμε στο γεγονός ότι καμία από τις δέκα εφαρμογές που μελετήθηκαν δεν παρουσιάζεται απόλυτα αξιόπιστη και σαφής προς το χρήστη. Καμία πολιτική ιδιωτικότητας δεν αναφέρθηκε σε όλες τις πτυχές που είναι αναγκαίο να σχολιαστούν, δηλαδή στο τι δεδομένα συλλέγει, πως τα συλλέγει, ποια είναι η χρήση τους, με τι σκοπό συλλέγονται, με ποιες τρίτες οντότητες η εκάστοτε εφαρμογή συνεργάζεται και αν διαμοιράζει προσωπικά δεδομένα με τις αυτές τρίτες οντότητες.
- ❖ Οι περισσότερες πολιτικές ιδιωτικότητας των εφαρμογών παρουσίασαν ελλείψεις, όμως αξίζει να αναφέρουμε ότι οι δυο πιο σαφείς, ως προς το χρήστη, πολιτικές ιδιωτικότητας, κρίθηκε ότι ήταν αυτές των εφαρμογών Facebook και WhatsApp. Από την άλλη πλευρά, οι πολιτικές ιδιωτικότητας που κρίθηκαν πιο αδύναμες και ελλιπείς, φαίνεται να είναι αυτές των εφαρμογών Mozilla Firefox και Google Chrome.
- ❖ Αναλυτικότερα, οι πιο ολοκληρωμένες πολιτικές ιδιωτικότητας φαίνεται ότι είναι των Facebook, Whats App και Netflix οι οποίες αναλύουν εκτενώς τα δεδομένα που συλλέγουν, τον σκοπό χρήσης αυτών καθώς και τις συνεργαζόμενες τρίτες οντότητες.
- ❖ Όσον αφορά την πολιτική ιδιωτικότητας του Twitter, δεν γίνεται καμία αναφορά στον τρόπο χρήσης των πληροφοριών που συλλέγει η εφαρμογή.

- ❖ Παράλληλα, οι ελλείψεις στην πολιτική ιδιωτικότητας του Viber, παρατηρούνται στην αποφυγή αναφοράς των τρόπων που συλλέγονται τα δεδομένα αλλά και των συνεργαζόμενων τρίτων οντοτήτων.
- ❖ Αναφορικά με την πολιτική ιδιωτικότητας του Stremio, θεωρείται ικανοποιητική, με μοναδική της αδυναμία την ελάχιστη αναφορά στους τρόπους χρήσης των δεδομένων που συλλέγονται από την εφαρμογή.
- ❖ Όσον αφορά την πολιτική ιδιωτικότητας της εφαρμογής Skype, θεωρείται ανεπαρκής καθώς η αναφορά της στα δεδομένα που συλλέγει είναι πολύ συνοπτική και ελλιπής.
- ❖ Παρομοίως, η πολιτική ιδιωτικότητας της εφαρμογής Zoom, ενώ κάνει αναφορά στη συλλογή των δεδομένων του χρήστη και στους τρόπους χρήσης αυτών, παραλείπει τον καθορισμό των συνεργαζόμενων τρίτων οντοτήτων, αντικείμενο πολύ σημαντικό για την προστασία της ιδιωτικότητας του χρήστη.
- ❖ Τέλος, οι πολιτικές ιδιωτικότητας των Mozilla Firefox και Google Chrome δεν αναφέρονται καθόλου στη συλλογή των δεδομένων των χρηστών, καθώς και ο σχολιασμός τους αναφορικά με τους σκοπούς χρήσης των δεδομένων είναι ανεπαρκής. Τα αποτελέσματα αυτά θα πρέπει να προκαλούν ιδιαίτερη ανησυχία στους αναγνώστες και χρήστες των εφαρμογών, καθώς αυτές οι δυο εφαρμογές χρησιμοποιούνται από όλους μας σε καθημερινή βάση.

6.Επίτευξη Στόχων Πτυχιακής και Μελλοντικές Προσθήκες

Ο στόχος της παρούσας πτυχιακής ήταν η κατάληξη σε αξιόπιστα συμπεράσματα, μελετώντας και αναλύοντας τις άδειες πρόσβασης των εφαρμογών Android του Google Play.

Ο σκοπός θεωρούμε πως επιτεύχθηκε με επιτυχία και οι αναγνώστες, λαμβάνοντας υπόψη τα αποτελέσματα και συμπεράσματα που δημιουργήθηκαν από την παρούσα εργασία, θα επιλέγουν ορθότερα το είδος των εφαρμογών που θα εγκαταστήσουν μελλοντικά.

Παράλληλα, στο δεύτερο μέρος της πτυχιακής, διερευνήθηκαν οι πολιτικές ιδιωτικότητας των δέκα πιο δημοφιλών εφαρμογών, όπου μετά από μελέτη, ορισμένες κρίθηκαν ανεπαρκείς προς το χρήστη.

Αναφορικά με τη συμβολή της παρούσας πτυχιακής στη βιβλιογραφία, αυτή είναι ορατή, καθώς η έρευνα, τα αποτελέσματα και τα συμπεράσματα της εργασίας αυτής, βοηθούν τον αναγνώστη και χρήστη να παρέχει με μεγαλύτερη συνέπεια τις άδειες πρόσβασης που του ζητούνται καθώς και να αποφασίζει με

μεγαλύτερη επιλεκτικότητα τις εφαρμογές του Google Play που επιθυμεί να εγκαταστήσει. Παράλληλα, η εργασία αυτή αποτελεί ένα βοηθητικό εργαλείο για τους ερευνητές που επιθυμούν να μελετήσουν μελλοντικά παρόμοιο ζήτημα αναφορικά με τις άδειες πρόσβασης.

Τα αποτελέσματα που δημιουργήθηκαν από την παρούσα πτυχιακή εργασία, είναι επαρκή για την εξαγωγή έγκυρων συμπερασμάτων, τόσο για τις πολιτικές ιδιωτικότητας των εφαρμογών που μελετήθηκαν, όσο και για τις άδειες πρόσβασης των εφαρμογών Android. Ωστόσο, αν κάποιος μελλοντικός ερευνητής θα ήθελε να εξελίξει περαιτέρω την παρούσα εργασία, θα μπορούσε να μελετήσει τις πολιτικές ιδιωτικότητας περισσότερων εφαρμογών. Ακόμα, θα μπορούσε να αντλήσει τα δεδομένα από όλες τις κατηγορίες του Google Play, έτσι ώστε να δημιουργηθούν ακόμα πιο έγκυρα και πλήρη αποτελέσματα.

Βιβλιογραφία

1. <https://www.macworld.co.uk/feature/iphone/iphone-vs-android-market-share-3691861/>
2. <https://el.wikipedia.org/wiki/Android>
3. <https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>
4. <https://academic.oup.com/sw/article-abstract/13/4/114/1872392?redirectedFrom=fulltext>
5. <https://www.amnesty.gr/universal-declaration-of-human-rights>
6. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
7. <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>
8. https://www.echr.coe.int/Documents/Convention_ELL.pdf
9. - <https://coinaccord.io/blog/three-ways-data-protection-laws-will-affect-blockchain-organizations>
10. <http://artemis.cslab.ece.ntua.gr:8080/jspui/handle/123456789/8692>

11. https://www.auth.gr/sites/default/files/gdpr_definitions_0.pdf
12. <https://www.w3.org/P3P/>
13. https://www.ebayinc.com/stories/news/ebay-inc-ask-ebay-users-change-passwords/?utm_source=301Redirect&utm_medium=301Redirect&utm_campaign=301Redirect
14. <https://theblog.adobe.com/important-customer-security-announcement/>
15. [https://en.wikipedia.org/wiki/Sony_Pictures_hack\](https://en.wikipedia.org/wiki/Sony_Pictures_hack)
16. <https://ir.homedepot.com/phoenix.zhtml?c=63646&p=iro1-newsArticle&ID=1987135>
17. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1141&context=amcis2014>
18. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
19. https://developer.android.com/reference/android/Manifest.permission.html#ACCESS_LOCATION_EXTRA_COMMANDS
20. <https://developer.android.com/guide/topics/permissions/overview>
21. <https://www.howtogeek.com/190863/androids-app-permissions-were-just-simplified-now-theyre-much-less-secure/>
22. http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9619/Tsavli_Matina.pdf?sequence=1&isAllowed=y
23. https://en.wikipedia.org/wiki/Microsoft_Visual_Studio
24. <https://www.facebook.com/about/privacy/>
25. <https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/>
26. <https://twitter.com/en/privacy>

27. <https://help.twitter.com/en/rules-and-policies/twitter-api>
28. <https://www.viber.com/en/terms/viber-privacy-policy/>
29. <https://www.whatsapp.com/legal?doc=privacy-policy&version=20160825>
30. <https://el.wikipedia.org/wiki/Netflix>
31. <https://help.netflix.com/legal/privacy>
32. <https://www.stremio.com/privacy>
33. <https://www.w3schools.com/browsers/default.asp>
34. <https://www.google.com/intl/en/chrome/privacy/>
35. <https://www.w3schools.com/browsers/>
36. <https://el.wikipedia.org/wiki/VoIP>
37. <https://www.skype.com/el/legal/>
38. <https://privacy.microsoft.com/el-gr/privacystatement>
39. <https://zoom.us/privacy>
40. <https://stackoverflow.com/questions/8305613/converting-int-to-real-in-sqlite/8305623>
41. <https://stackoverflow.com/questions/32953639/how-to-type-cast-in-sqlite3>
42. [Www.androidpermissions.com](http://www.androidpermissions.com)
43. Hoffman, C. (2015), “How to Manage App Permissions on Android 6.0”, <http://www.howtogeek.com/230683/how-to-manage-app-permissions-on-android-6.0/>
44. Johnson, R., Wang, Z., Gagnon, C., Stavrou, A. (2012), “Analysis android applications’ permissions”, In Proceedings of the 6th International Conference on Software Security and Reliability.
45. Rawan Baalous, Ronald Poet, How Dangerous Permissions are Described in Android Apps' Privacy Policies?, 2018, <https://dl.acm.org/citation.cfm?id=3264477>

46. <https://developer.android.com/guide/topics/permissions/overview>
47. <https://www.rewardle.com/permissions/android>
48. «EU General Data Protection Regulation (GDPR) : An Implementation and Compliance Guide», 2017
49. <https://www.poeota.gr/images/poe-ota-content/1625/fek-tefxos-v-186-2020-arxi-prostasias-dedomenon-prosopikou-xaraktira.pdf>
50. <https://openaccess.city.ac.uk/id/eprint/19741/>
(Abro, Fauzia Idrees,2018)
51. https://dl.acm.org/doi/abs/10.1145/2295136.2295141?casa_token=I9qynOR5EGwAAAAA:H3JCJWCKb3SrSs6YYP9Wn9AS_UkUkhKh-RMZiXY4DJkmiCHTx0od785xEp3bwcXdPLPk1Gurlg
52. A Proactive Approach toward Privacy Risk Assessment for Android Apps Permissions by Hamed, Ayed and Machfar (2017)
53. Automatically Granted Permissions in Android apps by Calciati and Kuznetsov (2020).

Παράρτημα Α

A/A	ΑΔΕΙΑ ΠΡΟΣΒΑΣΗΣ	ΠΕΡΙΓΡΑΦΗ ΑΔΕΙΑΣ
1	ACCESS_COARSE_LOCATION	Approximate location
2	ACCESS_FINE_LOCATION	Precise location
3	ACCESS_LOCATION_EXTRA_COMMANDS	Access extra location provider commands
4	ACCESS_MOCK_LOCATION	Allows a developer to create mock location in order to develop tests.
5	ACCESS_NOTIFICATION_POLICY	Marker permission for applications that wish to access notification policy.
6	ACCESS_SURFACE_FLINGER	Access SurfaceFlinger
7	ACCESS_WIFI_STATE	Wi-Fi Connection

8	ACCOUNT_MANAGER	Allows applications to call into AccountAuthenticators.
9	ACCESS_NETWORK_STATE	Network Connection
10	ADD_VOICEMAIL	Add Voicemail
11	ANSWER_PHONE_CALLS	Allows the app to answer phone calls
12	AUTHENTICATE_ACCOUNTS	Create accounts and set passwords
13	ACCESS_DOWNLOAD_MANAGER	Manage downloads
14	ACCEPT_HANDOVER	Allow a calling app to continue a call which was started in another app
15	ACCESS_CHECKIN_PROPERTIES	Read/write access to "properties" table in database.
16	BATTERY_STATS	Allows an app to collect battery statistics.
17	BIND_ACCESSIBILITY_SERVICE	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
18	BIND_APPWIDGET	Allow the app to choose Widget.
19	BIND_AUTOFILL_SERVICE	Must be required by an AutofillService, to ensure that only the system can bind to it.
20	BACKUP	Controls system's backup and restore.
21	BIND_CARRIER_SERVICES	The system process that is allowed to bind to services in carrier apps will have this permission.
22	BIND_CHOOSER_TARGET_SERVICE	Bind chooser target service.
23	BIND_CONDITION_PROVIDER_SERVICE	Must be required by a ConditionProviderService, to ensure that only the system can bind to it.
24	BIND_DEVICE_ADMIN	Must be required by device administration receiver, to ensure that only the system can interact with.
25	BIND_DREAM_SERVICE	Bind to a dream service.
26	BIND_INCALL_SERVICE	Bind to an incall service.
27	BIND_INPUT_METHOD	Bind to an input method.

28	<i>BIND_MIDI_DEVICE_SERVICE</i>	Bind to a midi device service.
29	<i>BIND_NFC_SERVICE</i>	Bind to a nfc service.
30	<i>BIND_NOTIFICATION_LISTENER_SERVICE</i>	Bind notification listener service.
31	<i>BIND_PRINT_SERVICE</i>	Bind to a print service.
32	<i>BIND_QUICK_SETTINGS_TILE</i>	Bind to a quick settings tile .
33	<i>BIND_REMOTEVIEWS</i>	Bind a widget service.
34	<i>BIND_SCREENING_SERVICE</i>	Bind screening service.
35	<i>BIND_TEXT_SERVICE</i>	Bind text service.
36	<i>BIND_TV_INPUT</i>	Bind tv input.
37	<i>BIND_VPN_SERVICE</i>	Bind vpn service.
38	<i>BIND_WALLPAPER</i>	Bind wallpaper.
39	<i>BLUETOOTH</i>	Allow applications to connect to paired Bluetooth devices.
40	<i>BLUETOOTH_ADMIN</i>	Allow applications to discover and pair Bluetooth devices.
41	<i>BLUETOOTH_PRIVILEGED</i>	Allows applications to pair Bluetooth devices without user interaction, and to allow or disallow phonebook access or message access.
42	<i>BODY_SENSORS</i>	Allows an application to access data from sensors that the user uses to measure what is happening inside their body, such as heart rate.
43	<i>BRICK</i>	Permanently disable phone.
44	<i>BROADCAST_PACKAGE_REMOVED</i>	Allows an application to broadcast a notification that an application package has been removed.
45	<i>BROADCAST_SMS</i>	Allows an application to broadcast an SMS receipt notification.
46	<i>BROADCAST_STICKY</i>	Allows an application to broadcast sticky intents.
47	<i>BROADCAST_WAP_PUSH</i>	Allows an application to broadcast a WAP PUSH receipt notification.

48	CALL_PHONE	<i>Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call.</i>
49	CALL_PRIVILEGED	<i>Allows an application to call any phone number, including emergency numbers, without going through the Dialer user interface for the user to confirm the call being placed.</i>
50	CAMERA	<i>Access to the camera</i>
51	CAPTURE_AUDIO_OUTPUT	<i>Allows an application to capture audio output.</i>
52	CAPTURE_SECURE_VIDEO_OUTPUT	<i>Allows an application to capture secure video output.</i>
53	CAPTURE_VIDEO_OUTPUT	<i>Allows an application to capture video output.</i>
54	CHANGE_COMPONENT_ENABLED_STATE	<i>Allows an application to change whether an application component (other than its own) is enabled or not.</i>
55	CHANGE_CONFIGURATION	<i>Allows an application to modify the current configuration, such as locale.</i>
56	CHANGE_NETWORK_STATE	<i>Allows applications to change network connectivity state.</i>
57	CHANGE_WIFI_MULTICAST_STATE	<i>Allows applications to enter Wi-Fi Multicast mode.</i>
58	CHANGE_WIFI_STATE	<i>Allows applications to change Wi-Fi connectivity state.</i>
59	CLEAR_APP_CACHE	<i>Allows an application to clear the caches of all installed applications on the device.</i>
60	CLEAR_APP_USER_DATA	<i>Allows an application to clear all the user's data on the device.</i>

61	CONTROL_LOCATION_UPDATES	Allows enabling/disabling location update notifications.
62	DELETE_CACHE_FILES	Old permission for deleting an app's cache files, no longer used.
63	DELETE_PACKAGES	Allows an application to delete packages.
64	DEVICE_POWER	This permission forces the device to sleep.
65	DIAGNOSTIC	Allows applications to read/write to diagnostic resources.
66	DISABLE_KEYGUARD	Allows applications to disable the keyguard/screen lock if it is not secure.
67	DUMP	Allows an application to retrieve state dump information from system services.
68	EXPAND_STATUS_BAR	Allows an application to expand or collapse the status bar.
69	FACTORY_TEST	Run as a manufacturer test application, running as the root user.
70	FLASHLIGHT	Control flashlight.
71	FORCE_BACK	Force an app to close.
72	FOREGROUND_SERVICE	Allows a regular application to use <u>Service.startForeground</u>.
73	GET_ACCOUNTS	Allows an app to access to the list of accounts.
74	GET_ACCOUNTS_PRIVILEGED	Allows an app to access to the list of accounts.
75	GET_PACKAGE_SIZE	Measure the storage space an app is using.
76	GET_TASKS	Retrieving running apps.
77	GET_TOP_ACTIVITY_INFO	Get current app info.
78	GLOBAL_SEARCH	This permission can be used on content providers to allow the global search system to access their data.
79	HARDWARE_TEST	Allows the app to control various peripherals for the

		purpose of hardware testing.
80	INJECT_EVENTS	Press keys and control buttons.
81	INSTALL_LOCATION_PROVIDER	Allows an application to install a location provider into the Location Manager.
82	INSTALL_PACKAGES	Allows an application to install packages.
83	INSTALL_SHORTCUT	Allows an application to install a shortcut in Launcher.
84	INSTANT_APP_FOREGROUND_SERVICE	Allows an instant app to create foreground services.
85	INTERNAL_SYSTEM_WINDOW	Allows an application to open windows that are for use by parts of the system user interface.
86	INTERNET	Allows applications to open network sockets.
87	KILL_BACKGROUND_PROCESSES	The system kills immediately all the background processes associated with the given package.
88	LOCATION_HARDWARE	Allows an application to use location features in hardware, such as the geofencing api.
89	MANAGE_ACCOUNTS	Add or remove accounts.
90	MANAGE_APP_TOKENS	Allows an application to manage (create, destroy) application tokens in the window manager.
91	MANAGE_DOCUMENTS	Allows an application to manage access to documents, usually as part of a document picker.
92	MANAGE_USB	Manage preferences and permissions for USB devices
93	MANAGE_USERS	Allows apps to manage users on the device, including query, creation and deletion.
93	MASTER_CLEAR	Reset system to factory defaults.

94	<i>MEDIA_CONTENT_CONTROL</i>	<i>Allows an application to know what content is playing and control its playback.</i>
95	<i>MODIFY_AUDIO_SETTINGS</i>	<i>Change your audio settings.</i>
96	<i>MODIFY_PHONE_STATE</i>	<i>Allows the app to control the phone features of the device. An app with this permission can switch networks, turn the phone radio on and off without ever notifying you.</i>
97	<i>MOUNT_FORMAT_FILESYSTEMS</i>	<i>Allows the app to format removable storage (SD card).</i>
98	<i>MOUNT_UNMOUNT_FILESYSTEMS</i>	<i>Allows the app to mount and unmount filesystems for removable storage (access SD Card filesystem).</i>
99	<i>MOVE_PACKAGE</i>	<i>Move app resources.</i>
100	<i>NFC</i>	<i>Allows the app to communicate with Near Field Communication (NFC) tags, cards, and readers.</i>
101	<i>NFC_TRANSACTION_EVENT</i>	<i>Allows applications to receive NFC transaction events.</i>
102	<i>PACKAGE_USAGE_STATS</i>	<i>Allows an application to collect component usage statistics.</i>
103	<i>PERSISTENT_ACTIVITY</i>	<i>Make an app always run.</i>
104	<i>PROCESS_OUTGOING_CALLS</i>	<i>Reroute outgoing calls. This permission allows the app to monitor, redirect, or prevent outgoing calls.</i>
105	<i>READ_ATTACHMENT</i>	<i>Allows the app to read your email attachments.</i>
106	<i>READ_CALENDAR</i>	<i>Allows the app to read all calendar events stored on your phone, including those of friends or co-</i>

		workers. This may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity.
107	<i>READ_CALL_LOG</i>	Allows the app to read your phone's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge.
108	<i>READ_CONTACTS</i>	Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals.
109	<i>READ_EXTERNAL_STORAGE</i>	Allows the app to read the contents of your removable storage (SD card).
110	<i>READ_FRAME_BUFFER</i>	Read the current frame buffer.
111	<i>READ_HISTORY_BOOKMARKS</i>	Allows the app to read the history of all URLs that the Browser has visited, and all of the Browser's bookmarks.
112	<i>READ_INPUT_STATE</i>	Allows an application to retrieve the current state of keys and switches.
113	<i>READ_LOGS</i>	Allow an application to read the low-level system file logs. This permission may includes personal information.
114	<i>READ_PHONE_NUMBERS</i>	Allows read access to the device's phone number(s).
115	<i>READ_PHONE_STATE</i>	Allows the app to access the phone features of the device.

116	READ_PROFILE	Allows the app to read personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others.
117	READ_SMS	Allows the app to read SMS messages stored on your phone or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality.
118	READ_SOCIAL_STREAM	Allows the app to access and sync social updates from you and your friends. This allows the app to read communications between people on social networks, regardless of confidentiality.
119	READ_SYNC_SETTINGS	Allow the app to read the sync settings for an account.
120	READ_SYNC_STATS	Allows an app to read the sync stats for an account, including the history of sync events and how much data is synced.
121	READ_USER_DICTIONARY	Allows the app to read all words, names and phrases that the user may have stored in the user dictionary.
122	READ_VOICEMAIL	Allows an application to read voicemails in the system.
123	REBOOT	Reboot
124	RECEIVE_BOOT_COMPLETED	Run at startup. Allows the app to have itself started as soon as the system has finished booting.
125	RECEIVE_MMS	Allows the app to receive and process MMS messages. This means the

		app could monitor or delete messages sent to a device without showing them to the user.
126	RECEIVE_SMS	Allows the app to receive and process SMS messages. This means the app could monitor or delete messages sent to a device without showing them to the user.
127	RECEIVE_WAP_PUSH	Allows the app to receive and process WAP messages. This means the app could monitor or delete messages sent to a device without showing them to the user.
128	RECORD_AUDIO	Allows the app to record audio with the microphone. This permission allows the app to record audio at any time without your confirmation.
129	REORDER_TASKS	Allows the app to move tasks to the foreground and background.
130	REQUEST_COMPANION_RUN_IN_BACKGROUND	Allows a companion app to run in the background.
131	REQUEST_COMPANION_USE_DATA_IN_BACKGROUND	Allows a companion app to use data in the background.
132	REQUEST_DELETE_PACKAGES	Allows an application to request deleting packages.
133	REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	Permission to ignore battery optimizations.
134	REQUEST_INSTALL_PACKAGES	Allows an application to request installing packages.
135	RESTART_PACKAGES	Allows the app to end background processes of other apps. This may cause other apps to stop running.
136	SEND_RESPOND_VIA_MESSAGE	Allows the app to send requests to other messaging apps to handle

		respond-via-message events for incoming calls.
137	SEND_SMS	Allows the app to send SMS messages. This may result in unexpected charges. Malicious apps may cost money , to the user by sending messages without his confirmation.
138	SET_ACTIVITY_WATCHER	Allows an application to watch and control how activities are started globally in the system.
139	SET_ALARM	Allows the app to set an alarm in an installed alarm clock app.
140	SET_ALWAYS_FINISH	Allows the app to control whether activities are always finished as soon as they go to the background.
141	SET_ANIMATION_SCALE	Allows the app to change the global animation speed (faster or slower animations) at any time.
142	SET_DEBUG_APP	Allows the app to turn on debugging for another app. Malicious apps may use this to kill other apps.
143	SET_ORIENTATION	Control screen orientation.
144	SET_POINTER_SPEED	Change pointer speed.
145	SET_PREFERRED_APPLICATIONS	Allows the app to modify your preferred apps. Malicious apps may silently change the apps that are run, spoofing the existing apps to collect private data from the user.
146	SET_PROCESS_LIMIT	Allows the app to control the maximum number of processes that will run.
147	SET_TIME	Allows applications to set the system time directly.
148	SET_TIME_ZONE	Allows the app to change the phone's time zone.
149	SET_WALLPAPER	Allows the app to set the system wallpaper.
150	SET_WALLPAPER_HINTS	Allows the app to set the system wallpaper size hints.

151	SHUTDOWN	Permission to shut down the device.
152	SIGNAL_PERSISTENT_PROCESSES	Allows the app to request that the supplied signal be sent to all persistent processes.
153	STATUS_BAR	Change the device status bar settings.
154	SUBSCRIBED_FEEDS_READ	Allows the app to get details about the currently synced feeds.
155	SUBSCRIBED_FEEDS_WRITE	Allows the app to modify your currently synced feeds. Malicious apps may change your synced feeds.
156	SYSTEM_ALERT_WINDOW	Allows the app to draw on top of other applications or parts of the user interface.
157	TRANSMIT_IR	Allows the app to use the phone's infrared transmitter.
158	UNINSTALL_SHORTCUT	Allows the application to remove Homescreen shortcuts without user intervention.
159	UPDATE_DEVICE_STATS	Update device statistics.
160	USE_BIOMETRIC	Allows an app to use device supported biometric modalities.
161	USE_CREDENTIALS	Allows the app to request authentication tokens.
162	USE_FINGERPRINT	Allows an app to use fingerprint hardware.
163	USE_SIP	Allows the app to use the SIP service to make/receive Internet calls.
164	VIBRATE	Allows the app to control the vibrator.
165	WAKE_LOCK	Allows the app to prevent the phone from going to sleep.
166	WRITE_APN_SETTINGS	Allows the app to change network settings and to intercept and inspect all network traffic, for example to change the proxy and port of any APN. Malicious apps

		<i>may monitor, redirect, or modify network packets without the user's knowledge.</i>
167	WRITE_CALENDAR	<i>Allows the app to add, remove, change events that a user can modify on his phone, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owner's , or modify events without the owners' knowledge.</i>
168	WRITE_CALL_LOG	<i>Allows the app to modify user's phone's call log, including data about incoming and outgoing calls. Malicious apps may use this to erase or modify the user's call log.</i>
169	WRITE_CONTACTS	<i>Allows the app to modify the data about user's contacts stored on the device, including calls and emails. This permission allows apps to delete contact data.</i>
170	WRITE_EXTERNAL_STORAGE	<i>Allows the app to write to the removable storage (SD card).</i>
171	WRITE_GSERVICES	<i>Allows an application to modify the Google service map.</i>
172	WRITE_HISTORY_BOOKMARKS	<i>Allows the app to modify the Browser's history or bookmarks stored on user's phone. This may allow the app to erase or modify Browser data.</i>
173	WRITE_PROFILE	<i>Allows the app to change or add to personal profile information stored on user's device, such as name and contact information. This means the app can identify the user and may send his</i>

		<i>profile information to others.</i>
174	WRITE_SECURE_SETTINGS	<i>Allows the app to modify the system's secure settings data.</i>
175	WRITE_SETTINGS	<i>Change or modify system settings.</i>
176	WRITE_SMS	<i>Allows the app to write to SMS messages stored on the user's phone or SIM card. Malicious apps may delete messages.</i>
177	WRITE_SOCIAL_STREAM	<i>Allows the app to display social updates from the user's friends.</i>
178	WRITE_SYNC_SETTINGS	<i>Toggle sync on and off. Allows an app to modify the sync settings for an account.</i>
179	WRITE_USER_DICTIONARY	<i>Allows the app to write and add new words into the user dictionary.</i>
180	WRITE_VOICEMAIL	<i>Write voicemails</i>