ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

<<Τα κοινωνικά δίκτυα και η ιδιωτικότητά τους>>

Της φοιτητριας

Καρφοπούλου Κωνσταντίνας

Αρ. Μητρώου: 06/3100

Επιβλέπων καθηγητής

Ηλιούδης Χρήστος

Θεσσαλονίκη 2012

ΠΕΡΙΛΗΨΗ

Η πτυχιακή εργασία πραγματεύεται τα κοινωνικά δίκτυα και την ιδιωτικότητά τους, έχοντας ως στόχο την ανάλυση της αξίας της ιδιωτικότητας, κατά την διάρκεια της πλοήγησης των χρηστών στους συγκεκριμένους ιστότοπους. Πραγματοποιείται εκτενή αναφορά παραδειγμάτων παραβίασης της ιδιωτικότητας των χρηστών, ενώ στη συνέχεια παραθέτονται λεπτομερώς βασικοί κίνδυνοι και απειλές. Ακολουθούν υποδείξεις και συμβουλές, που σκοπό έχουν την αποφυγή των κινδύνων αυτών, καθώς επίσης και την προφύλαξη από αυτούς. Επιπλέον παρουσιάζεται μια συγκριτική αξιολόγηση των μηχανισμών και πολιτικών προστασίας της ιδιωτικότητας για τα τρία πιο γνωστά κοινωνικά δίκτυα Facebook, το Twitter και το Google+. Τέλος, παραθέτονται αξιοσημείωτες προτάσεις και συμβουλές τόσο προς τους χρήστες των ιστοσελίδων κοινωνικής δικτύωσης, όσο και προς τα ίδια τα κοινωνικά δίκτυα, στοχεύοντας έτσι στην βέλτιστη προστασία της ιδιωτικότητας των χρηστών.

ABSTRACT

The project (thesis) deals with social networks and their privacy, aiming to analyze the value of privacy during the navigation of users on these specific sites. Extensive reference to examples of violation of the privacy of users is made and then key risks and threats are explained in detail. Hints and tips follow, aimed at the avoidance of these risks, as well as the protection from them. Next, the three most popular social networks, Facebook, Twitter and Google + are presented, each with its own privacy policy. Finally, notable suggestions and tips for users of social networking sites are listed, addressed to both the users of social network web pages as well as to the social networks themselves, thus aiming to optimize the protection of the privacy of users.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευρετήριο σχημάτων

Ευρετήριο πινάκων

Κεφάλαιο 1: Τα κοινωνικά δίκτυα

1.1 Σκοπός και στόχοι της πτυχιακής εργασίας

Στην εποχή που ζούμε, η χρήση του διαδικτύου αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας όλων σχεδόν των ανθρώπων. Ταυτόχρονα, όμως με την χρήση του διαδικτύου, μέγαλη εξέλιξη έχουν γνωρίσει και οι ιστοσελίδες κοινωνικής δικτύωσης. Πλήθος χρηστών ξοδεύει αρκετό απο τον χρόνο του στους ιστότοπους των κοινωνικών δικτύων. Ωστόσο, η ανησυχία των ίδιων για την διαχείριση των ιδιωτικών τους δεδομένων και πληροφοριών βρίσκεται συνεχώς στην επικαιρότητα. Στην παρούσα πτυχιακή εργασία ερευνούμε τους κινδύνους και τις απειλές, που στρέφονται εναντίον της ιδιωτικότητας και αναλύουμε μια ποικιλία παραδειγμάτων, κατά τα οποία οι χρήστες βρίσκονται στο ρόλο του θύματος. Προσπαθούμε να προτείνουμε βασικές οδηγίες και συμβουλές, οι οποίες στόχο έχουν την επίλυση αυτού του προβλήματος, που θίγει στις μέρες μας την πλειοψηφία των χρηστών του διαδικτύου. Σκοπός της συγκεκριμένης εργασίας είναι να μεταδώσει στους αναγνώστες της μία εικόνα της αξίας της ιδιωτικότητας, καθώς επίσης και τους τρόπους διαφύλαξής της. Αφού ολοκληρωθεί η παρούσα πτυχιακή εργασία, στοχεύουμε στην πλήρη και αντικειμενική ενημέρωση των χρηστών και μη των κοινωνικών δικτύων, σχετικά με το πρόβλημα της παραβίασης της ιδιωτικότητας κατά την πλοήγησή τους στις ιστοσελίδες αυτές. Απώτερος σκοπός, μετά το πέρας της εργασίας, είναι οι χρήστες να αναπτύξουν ακόμη περισσότερο την γνώση τους και την ενημέρωση τους, για μια πιο ασφαλή ενασχόληση με τα κοινωνικά δίκτυα.

1.2 Ορισμός και είδη κοινωνικών δικτύων

1.2.1 Ορισμοί

Κατά καιρούς, έχουν δοθεί διάφοροι ορισμοί γύρω απο την έννοια των κοινωνικών δικτύων. Ένας απο τους πιο επικρατέστερους είναι αυτός, που έχει δοθεί από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA 2011), όπου αφορά ψηφιακές κοινότητες που - μέσω της δημιουργίας ενός προφίλ (profile) - επιτρέπουν στους ανθρώπους, να συναντιούνται, να επικοινωνούν, να παραμένουν σε επαφή, να μοιράζονται φωτογραφίες και εικόνες με άλλα μέλη της κοινότητας. Σε γενικές γραμμές, ένα κοινωνικό δίκτυο αποτελεί μία κοινωνική δομή αποτελούμενη από άτομα, που ονομάζονται κόμβοι και συνδέονται με έναν ή περισσότερους τύπους αλληλεξάρτησης, όπως φιλίας, σεξουαλικών σχέσεων, κοινών πεποιθήσεων κλπ. (Πάσσας 2009)

1.2.2 Είδη Κοινωνικών δικτύων

Αναλυτές προσπάθησαν κατά καιρούς να διαχωρίσουν τα διάφορα κοινωνικά δίκτυα σε κατηγορίες. Ένας πρώτος διαχωρισμός αναφέρεται μεταξύ στα ολοκληρωμένα ή πλήρη κοινωνικά δίκτυα και στα προσωπικά ή εγωκεντρικά δίκτυα. Αναλυτικότερα, όταν αναφερόμαστε στα ολοκληρωμένα - πλήρη δίκτυα ουσιαστικά μελετάμε τις σχέσεις που αναπτύσσονται μέσα σε έναν συγκεκριμένο πληθυσμό (Παπανικολάου 2011). Απο την άλλη μεριά, στα προσωπικά - εγωκεντρικά δίκτυα μελετάμε όλους εκείνους τους δεσμούς που αναπτύσσουν οι άνθρωποι μέσα σε συγκεκριμένες κοινότητες. Ουσιαστικά, οι αναλυτές εξετάζουν τις σχέσεις που δημιουργεί ένα άτομο (ego), που είναι και ο κεντρικός μας παράγοντας, προς τα υπόλοιπα άτομα με τα οποία συνδέεται (alters). Επίσης, τα πλήρη δίκτυα σε σχέση με τα εγωκεντρικά διαχωρίζονται και ως προς το μέγεθός τους. Στα προσωπικά δίκτυα συναντάμε το πολύ εκατόν πενήντα μέλη, όριο το οποίο προτάθηκε απο τον αναλυτή Robin Dunbar (Robin Ian MacDonald Dunbar 2011).

1.3 Υπηρεσίες Κοινωνικών δικτύων και μικρή ιστορική αναδρομή

Οι υπηρεσίες κοινωνικής δικτύωσης αποτελούν διαδικτυακές υπηρεσίες που επιτρέπουν στους χρήστες να διατηρούν ένα δημόσιο προφίλ να διαρθρώνουν και να αναπτύσσουν το δίκτυο επαφών τους και να μοιράζονται ψηφιακό περιεχόμενο. Από τα πρώτα χρόνια διάδοσης της έννοιας των κοινωνικών δικτύων, οι χρήστες ξεκίνησαν να δείχνουν μεγάλο ενδιαφέρον προς αυτά. Από τις πρώτες ιστοσελίδες κοινωνικής δικτύωσης, όπως για παράδειγμα Geocities.com (1994), Theglobe.com (1995), οι διαχειριστές αυτών ενθάρρυναν τους χρήστες να ανταλλάσσουν προσωπικές ιδέες και απόψεις μέσω των "δωματίων συνομιλιών" τα γνωστά δηλαδή σε όλους μας και ως chat rooms. Νέες ιστοσελίδες κοινωνικής δικτύωσης άρχισαν να εμφανίζονται όλο και συχνότερα, επιτρέποντας τους χρήστες να διαχειρίζονται λίστες απο συγκεκριμένα άτομα, που ήθελαν να επικοινωνήσουν, όπως επίσης να αναζητούν και νέους "φίλους" με συγκεκριμένα ενδιαφέροντα. Η νέα γενιά αυτή κοινωνικών δικτύων άρχισε να δείχνει τα πρώτα δείγματα άνθισης απο το 1997 και την εμφάνιση του δικτύου SixDegrees.com. Στη συνέχεια ακολούθησαν ιστοσελίδες κοινωνικής δικτύωσης όπως το Makeoutclub.com (2000), το Friendster.com (2002), το MySpace.com, το LinkedIn.com κλπ. Η μεγάλη έκρηξη, όμως των κοινωνικών δικτύων πραγματοποιήθηκε το 2004 με την εμφάνιση του Facebook (Παπαβασιλείου, Ραπτοπούλου 2011) . Στην αρχή είχε την μορφή ενός κλειστού ιστοχώρου για εκείνους που ανήκαν στην ακαδημαϊκή κοινότητα του Harvard.Τον Σεπτέμβριο του 2005, ανοίγει τις υπηρεσίες στο ευρύ κοινό του διαδικτύου με αποτέλεσμα να αριθμεί σήμερα περισσότερους απο 350 εκατομμύρια χρήστες. Περισσότερες απο 700 χιλιάδες εταιρείες στην Αμερική έχουν σελίδες στο facebook. Επίσης περισσότεροι απο 65 εκατομμύρια χρήστες χρησιμοποιούν το facebook μέσω κινητών συσκευών. Υπάρχουν όμως κάποιοι περιορισμοί. Ένας νέος χρήστης δεν συνδέεται ελεύθερα στα υπάρχοντα δίκτυα φίλων και αυτό το χαρακτηριστικό το διαφοροποιεί απο τα κοινωνικά δίκτυα που υπήρχαν μέχρι εκείνη την στιγμή. Ένα είδος κοινωνικών δικτύων που έχει γνωρίσει τεράστια ανάπτυξη, είναι αυτά τα οποία διαφοροποιούνται σε σχέση με τις υπηρεσίες που παρέχουν. Σε αυτά τα δίκτυα επιτρέπεται ο διαμοιρασμός φωτογραφιών, βίντεο, ειδήσεων, συζητήσεων κλπ. Το διαφορετικό σε

αυτή την περίπτωση από τις άλλες μορφές εικονικών κοινοτήτων αναφέρεται στο γεγονός, ότι οι χρήστες μπορούν να κάνουν ορατές τις προσωπικές τους συνδέσεις. Δηλαδή, οι συνδέσεις του ενός γίνονται πιθανές συνδέσεις του άλλου. Υπάρχουν συνδέσεις διπλής κατεύθυνσης ή συνδέσεις φίλων που απαιτείται συναίνεση σύνδεσης και απο τους δύο χρήστες. Επίσης υπάρχουν συνδέσεις μονής κατεύθυνσης ή συνδέσεις οπαδών, όπου οι χρήστες ακολουθούν κάποιον.

1.4 Κοινωνικά δίκτυα και χρήστες

1.4.1 Η καθημερινή αλληλεπίδραση

Οι περισσότεροι χρήστες κοινωνικών δικτύων έχουν καθημερινή επαφή και αλληλεπίδραση με αυτά. Τα δίκτυα αυτά έχουν εδραιωθεί εξαιτίας, τόσο του περιεχομένου που ίδιοι οι χρήστες κοινοποιούν, όσο και των δραστηριοτήτων τους. Όσους περισσότερους χρήστες διαθέτει ένα δίκτυο, τόσο πιο διάσημο χαρακτηρίζεται. Επιπλέον, η δημιουργία οποιασδήποτε κοινότητας δεν αποτελεί μόνο κοινωνικό χαρακτηριστικό των δικτύων, αλλά αποτελεί αναγκαία δραστηριότητα για την οποιαδήποτε χρήση υπηρεσιών και εφαρμογών. Από την άλλη μεριά, η επικοινωνία και η αλληλεπίδραση μεταξύ των χρηστών εκτείνονται σε πραγματικό χρόνο (real time), αλλά και σε μία διάσταση συγκεκριμένου τόπου. Για να γίνουμε πιο συγκεκριμένοι, οι υπηρεσίες εντοπισμού των χρηστών, καθώς επίσης και η δημιουργία ενός περιβάλλοντος ανοιχτής ενημέρωσης καθιστούν δυνατό στον χρήστη να γνωρίζει, αφενός που βρίσκονται οι φίλοι, αφετέρου σε ποια δραστηριότητα ή γεγονός έλαβαν συμμετοχή. Άλλωστε, ιδιαίτερο ενδιαφέρον φαίνεται να έχουν και οι στατιστικές μετρήσεις που έχουν πραγματοποιηθεί από εταιρεία του εξωτερικού, γνωστή και με το όνομα "InSites Consulting". Σύμφωνα λοιπόν με διάφορες έρευνες, το 66% των Ελλήνων μπαίνει στο διαδίκτυο καθημερινά, την στιγμή που ο ευρωπαϊκός μέσος όρος αγγίζει το 53%. Επιπλέον, ο αριθμός των Ελλήνων χρηστών, οι οποίοι έχουν δημιουργήσει λογαριασμό, σε κάποια απο τις ιστοσελίδες κοινωνικής δικτύωσης, φτάνει το 63%, σε αντίθεση

βέβαια με το ευρωπαϊκό ποσοστό, το οποίο ανέρχεται στο 45%. Τέλος, από το σύνολο των ενεργών χρηστών το 33% ανανεώνει το προφίλ του καθημερινά, ενώ το 37% παρακολουθεί σε καθημερινή βάση τα προφίλ των "φίλων" του.

1.4.2 Η διάδοση των κοινωνικών δικτύων στους Έλληνες χρήστες

Παρατηρώντας λοιπόν και τα παραπάνω νούμερα, είναι φανερό πως οι αριθμοί μπορούν να μιλήσουν απο μόνοι τους. Πιο αναλυτικά, στο ενάμισι εκατομμύριο ανέρχονται οι Έλληνες ενεργοί χρήστες στο κοινωνικό δίκτυο Facebook, ενώ σε περίπου τριακόσιους σαράντα χιλιάδες Έλληνες υπολογίζονται οι ενεργοί χρήστες του YouTube και σε ακόμα λιγότερους - 85 χιλιάδες περίπου - οι ενεργοί χρήστες του κοινωνικού δικτύου Twitter. Αυτό διαπιστώνεται από αναλυτικά στοιχεία μέτρησης της εταιρείας ηλεκτρονικής αποδελτίωσης InNews A.E.(franchise Ssuccess Team 2011). Οι παραπάνω αριθμοί προέκυψαν απο μελέτες που πραγματοποιήθηκαν κατά το δεύτερο και το τρίτο τρίμηνο του 2011. Σύμφωνα με τη μέτρηση, οι Έλληνες χρήστες του κοινωνικού δικτύου Twitter είναι οι πιο δραστήριοι. Αναφορές που αγγίζουν τις 180.000 (Tweets) ημερησίως αναρτούν οι Έλληνες, δηλαδή κατά μέσο όρο αντιστοιχούν περισσότερες από δύο αναφορές ημερησίως ανά χρήστη. Με ρυθμό περίπου μία αναφορά την εβδομάδα ανεβάζουν οι χρήστες τις αναφορές στα δύο άλλα κοινωνικά δίκτυα, το Facebook και το YouTube. Πιο συγκεκριμένα οι Έλληνες χρήστες του Facebook αναρτούν 240.000 αναφορές μέσα σε μία ημέρα (status updates & comments) και 50.000 αναφορές οι χρήστες του YouTube (comments & videos). Ο εθισμός των Ελλήνων στο φαινόμενο εξάπλωσης των κοινωνικών δικτύων είναι σχεδόν τρομακτικός. Δυστυχώς, τα νούμερα αυτά ξεπερνούν κατά πολύ τα όρια μίας λογικής χρήσης των ιστοσελίδων αυτών. Το πιο σημαντικό όμως, είναι ότι ο εθισμός των Ελλήνων χρηστών έχει προσβάλλει και τους εφήβους. Η χρήση διαδικτύου είναι εξαιρετικά δημοφιλής στους Έλληνες εφήβους και ενδέχεται να οδηγήσει σε ψυχοκοινωνικά προβλήματα, όταν υπάρχει υπερβολική χρήση. Η Μονάδα Εφηβικής Υγείας της Παιδιατρικής πανεπιστημιακής κλινικής του Νοσοκομείου Παίδων «Αγλαΐα Κυριακού» πραγματοποίησε μία πολύ σημαντική έρευνα σε εφήβους μεταξύ δεκαπέντε και δεκαέξι ετών και κατέληξε σε

συγκεκριμένα αποτελέσματα. Σύμφωνα λοιπόν με αυτά, αφ'ενός και έχει αυξηθεί υπερβολικά το ποσοστό χρήσης του διαδικτύου απο τους Έλληνες έφηβους, αφ'ετέρου το ποσοστό αυτό είναι ακόμη μεγαλύτερο στις επαρχιακές πόλεις, σε αντίθεση με τον πληθυσμό της Αττικής. Ακόμη, τα παιδιά με συμπεριφορές εξάρτησης, παρουσιάζουν στατιστικά σημαντική διαφορά στη χαμηλή βαθμολογία σχολείου σε σύγκριση με τους εφήβους που ασχολούνται με το διαδίκτυο σε φυσιολογικά πλαίσια. Εξάλλου, τα παιδιά με συμπεριφορές εξάρτησης επιδίδονται σε παιχνίδια τύχης και χρησιμοποιούν υλικό με σεξουαλικό περιεχόμενο σημαντικά συχνότερα από τα υπόλοιπα παιδιά. Μια πολύ σημαντική παρατήρηση αναφέρεται στο γεγονός, οτι την χρονιά 2007 πρώτοι στην κατηγορία εθισμού ήταν, τόσο τα αγόρια, όσο και τα διαδικτυακά παιχνίδια. Σήμερα, η διαφορά μεταξύ αγοριών και κοριτσιών έχει πλέον εξισορροπηθεί και την θέση των διαδικτυακών παιχνιδιών έχουν πάρει τα κοινωνικά δίκτυα. Η Μονάδα Εφηβικής Υγείας από το καλοκαίρι του 2007 έχει δεχθεί εφήβους με στόχο την αντιμετώπιση της υπερβολικής χρήσης τους διαδικτύου. Συνολικά εκατόν πενήντα έφηβοι έχουν απευθυνθεί στη μονάδα. Σε πρώιμα στάδια το φαινόμενο αντιμετωπίζεται σχετικά εύκολα με ψυχοεκπαίδευση. Σε προχωρημένο στάδιο εθισμού, ο έφηβος δεν αναγνωρίζει ότι υπάρχει πρόβλημα, δεν συνεργάζεται, μπορεί να λέει ψέματα και μπορεί να εξαπατά γονείς και θεραπευτές. Η συμπεριφορά του θυμίζει ατόμου εξαρτημένου από ουσίες. Το πρόβλημα εθισμού στα κοινωνικά δίκτυα, όταν αυτό συναντάται κυρίως σε παιδιά εφηβικής ηλικίας, μπορεί να επιφέρει δραματικές συνέπειες. Τόσο οι γονείς, όσο και οι εκπαιδευτικοί, θα πρέπει να είναι σωστά ενημερώμενοι και να γνωρίζουν το χρόνο κατά τον οποίο τα παιδιά τους χρησιμοποιούν τις ιστοσελίδες κοινωνικής δικτύωσης και να επιβάλλουν όρια, όταν αυτό απαιτείται.

1.5 Βασικοί κίνδυνοι

Αρχικά, τα κοινωνικά δίκτυα ξεκίνησαν ως μία έκφραση των νέων να συνομιλούν, να ανταλλάζουν απόψεις και ιδέες , να αποκτούν καινούργιους φίλους αλλά και να βρίσκουν παλαιότερους που έχουν καιρό να τους συναντήσουν. Η διάδοση των ιστοσελίδων κοινωνικής δικτύωσης έγινε αστραπιαία αφού μπορεί να γίνει απο

οποιοδήποτε σημείο και χωρίς κανένα κόστος, αρκεί φυσικά να υπάρχει πρόσβαση στο διαδίκτυο είτε μέσω Η/Υ, είτε μέσω κινητού τηλεφώνου, είτε ακόμη και μέσω συσκευών που επιτρέπουν την πρόσβαση στο διαδίκτυο (tablets) . Απο την άλλη μεριά, υπάρχουν και πολλές αντιδράσεις για την ¨ έξαρση ¨ των κοινωνικών δικτύων, καθώς τόσο η ιδιωτικότητα όσο και η προστασία προσωπικών δεδομένων είναι προβλήματα όπου η λύση τους εκκρεμεί. Το σίγουρο είναι, ότι η κοινωνία στην οποία ζούμε εξελίσσεται μέρα με την μέρα και οι τεχνολογικές αλλαγές επηρεάζουν την καθημερινή μας ζωή και θετικά αλλά και αρνητικά και είναι αναπόφευκτο γεγονός, πως ζούμε σε μία ψηφιακή εποχή. Ας δούμε, όμως αναλυτικότερα ποιοι είναι οι βασικοί κίνδυνοι, οι οποίοι κρύβονται πίσω απο τις ιστοσελίδες κοινωνικής δικτύωσης. Πρώτα από όλα να αναφέρουμε πως οι χρήστες κοινωνικών δικτύων, όπως για παράδειγμα το Facebook, δημιουργούν προφίλ, ανεβάζουν προσωπικές τους φωτογραφίες, εκφράζουν πολιτικές αλλά και θρησκευτικές ιδεολογίες και απόψεις, αποκαλύπτουν προσωπικά τους στοιχεία, όπως η ημερομηνία γέννησης, το φύλλο τους, τις σεξουαλικές τους προτιμήσεις ακόμη και το μέρος που παραβρίσκονται κάποια συγκεκριμένη χρονική στιγμή. Όλα τα παραπάνω, όπως είναι φανερό αποτελούν ευαίσθητα προσωπικά δεδομένα τα οποία πολλοί χρήστες αδυνατούν να προστατέψουν και αυτό συνήθως συμβαίνει λόγω άγνοιας του κινδύνου, αλλά πολλές φορές και εξαιτίας των ελλιπών γνώσεων απέναντι στην χρήση του διαδικτύου. Η προστασία των προσωπικών μας δεδομένων, όπως επίσης και της ιδιωτικότητας μας αποτελούν τα δομικά στοιχεία μιας σύγχρονης και δημοκρατικής κοινωνίας. Δυστυχώς όμως και οι δύο αυτές έννοιες έχουν τεθεί υπο αμφισβήτηση εξαιτίας του ισχύοντος νομοθετικού πλαισίου τόσο της χώρας μας όσο και της ίδιας της Ευρωπαϊκής Ένωσης. Δυστυχώς, ο αριθμός των κινδύνων μέσα σε ένα κοινωνικό δίκτυο είναι τεράστιος και όσο και αν οι χρήστες βρίσκουν πιθανές και προσωρινές λύσεις για τους υπάρχοντες, όλο και πιο σοβαροί εμφανίζονται με γεωμετρικό ρυθμό. Οι περισσότεροι κίνδυνοι θα αναλυθούν εκτενέστερα στα επόμενα κεφάλαια και ιδιαίτερη έμφαση θα δοθεί σε αυτούς, που αφορούν την ιδιωτικότητα των χρηστών. Βέβαια, δεν πρέπει σε καμία περίπτωση να θεωρηθεί, ότι οι υπόλοιποι κίνδυνοι, είτε αυτοί είναι παραδοσιακοί, είτε είναι κοινωνικής φύσεως απαιτούν λιγότερη σημασία και προσοχή. Απλά, τα κοινωνικά δίκτυα και οι κίνδυνοι γύρω από την ιδιωτικότητα των χρηστών είναι το αντικείμενο της συγκεκριμένης εργασίας.

1.6 Οργάνωση κειμένου

Στο επόμενο κεφάλαιο, παρουσιάζεται μία προσέγγιση της έννοιας της ιδιωτικότητας στο διαδίκτυο. Μετά απο διάφορους ορισμούς που δόθηκαν κατά καιρούς, καταλήγουμε σ' αυτόν που θεωρούμε ότι περιγράφεται καλύτερα η σημασία του όρου. Έπειτα, γίνεται περιγραφή των πιο χαρακτηριστικών παραδειγμάτων παραβίασης της ιδιωτικότητας, καθώς επίσης και πιθανοί τρόποι αντιμετώπισης του προβλήματος αυτού. Στο τρίτο κεφάλαιο τώρα, επιχειρείται μία θεωρητική προσέγγιση των πιο βασικών κινδύνων κατά της ιδιωτικότητας, αλλά και των υπολοίπων κινδύνων που εγκυμονούν μέσα στις ιστοσελίδες κοινωνικής δικτύωσης. Στο ίδιο κεφάλαιο, παρουσιάζονται αναλυτικά και προτεινόμενες λύσεις, οι οποίες στόχο έχουν να αφανίσουν ή έστω να περιορίσουν τους υπάρχοντες κινδύνους και απειλές. Στο τέταρτο κεφάλαιο, συγκεκριμενοποιούμε την έρευνα μας και σας παραθέτουμε τις πολιτικές απορρήτου, μερικών απο τα πιο διάσημα κοινωνικά δίκτυα. Επίσης, στην ενότητα αυτή συναντάμε και τις επιλογές που διαθέτει ο κάθε χρήστης, έτσι ώστε να ρυθμίσει το προσωπικό του λογαριασμό σύμφωνα με τις επιθυμίες του. Στο πέμπτο κεφάλαιο, περιγράφεται λεπτομερώς οι τρόποι σύμφωνα με τους οποίους ένα κοινωνικό δίκτυο μπορεί να διαμορφωθεί, πετυχαίνοντας έτσι την βέλτιστη προστασία της ιδιωτικότητας. Στη συνέχεια, προτείνουμε ακόμη βασικές συμβουλές και καθοδηγήσεις προς τους ίδιους τους χρήστες, που σκοπεύουμε να τις υιοθετήσουν προς όφελός τους. Στο έκτο και τελευταίο κεφάλαιο, διαμορφώνονται συγκεκριμένα συμπεράσματα για την ιδιωτικότητα των χρηστών στα κοινωνικά δίκτυα, όπως επίσης επεκτάσεις και προτάσεις για μελλοντική έρευνα.

Κεφάλαιο 2: Παραδείγματα παραβίασης της ιδιωτικότητας

2.1 Σημασία της ιδιωτικότητας

Με την ανάπτυξη του διαδικτύου και την ταυτόχρονη διάδοση των κοινωνικών δικτύων, συχνά γίνεται λόγος για την αξία της ιδιωτικότητας. Η έννοια της ιδιωτικότητας είναι τόσο ενδιαφέρουσα, όσο και μυστηριώδης, αφού σχεδόν κανένας δεν συμφωνεί στο τι πραγματικά είναι και εκφράζει. Πολλοί είναι αυτοί που συμφώνησαν, ότι η ιδιωτικότητα αποτελεί μία άκρως σημαντική ανθρώπινη αξία, απαραίτητη για πολλές εκφάνσεις της ηθικής και κοινωνικής πλευράς ενός ατόμου. Ενδεικτικές αναφορές για την ιδιωτικότητα, όπως ότι είναι ένα σημαντικό στοιχείο της προσωπικότητας και της ακεραιότητας (Fried 1968), αποτελεί προυπόθεση για την ανθρώπινη αξιοπρέπεια και διατηρεί την ατομικότητα και την αυτονομία του ατόμου (Bloustein 1964), είναι αναγκαία συνθήκη για την επίτευξη οικειότητας (Gerstein 1978) και τέλος αποτελεί απαραίτητη προυπόθεση για την ανάπτυξη διαφορετικών και βαρυσήμαντων σχέσεων (Rachles 1975). Λόγω όμως του γεγονότος, ότι η ιδιωτικότητα είναι μία σύνθετη και πολύπλοκη έννοια για να αποδοθεί με έναν μόνο και απλό ορισμό, οι περισσότεροι θεωρητικοί πρότειναν να αντιμετωπιστεί σαν συλλογή απο αλληλοσχετιζόμενες έννοιες. Έτσι, η ιδιωτικότητα αποτελεί μία ευρεία κοινωνική έννοια σύμφωνα με την οποία ένα άτομο αλληλεπιδρά και αντιλαμβάνεται την κοινωνία (Ben - Gauss 1983). Στις μέρες μας, σχεδόν όλοι οι χρήστες του διαδικτύου έχουν επαφή με τις ιστοσελίδες κοινωνικής δικτύωσης, άλλοι περισσότερο, άλλοι πάλι λιγότερο. Παρόλ'αυτα, πολλοί είναι αυτοί που αγνοούν τις επιπτώσεις που μπορεί να επιφέρει η παραβίαση της ιδιωτικότητάς τους μέσα στα κοινωνικά δίκτυα αυτά. Παρακάτω, θα γίνει μία αναφορά απο παραδείγματα παραβίασης της ιδιωτικότητας των χρηστών και θα αναλυθεί η σημασία και η αξία τόσο της πρόληψης, όσο και των τρόπων προστασίας απο πιθανούς κινδύνους.

2.2 Παραδείγματα παραβίασης της ιδιωτικότητας

Συχνό είναι το φαινόμενο, όπου κατά την σύνδεση ενός μέλους σε ένα οποιοδήποτε κοινωνικό δίκτυο, ο παροχέας του δικτύου αυτού εκτός απο τις απαραίτητες πληροφορίες σύνδεσης (όνομα χρήστη - κωδικός πρόσβασης) αποκτά πρόσβαση και σε άλλες δευτερεύουσες πληροφορίες. Έτσι, η παραβίαση της ιδιωτικότητας είναι γεγονός, αφού πληροφορίες προφίλ, η διεύθυνση του πρωτοκόλλου του διαδικτύου (ip address), συγκεντρωτικά δεδομένα χρηστών, αλλά και ο τύπος του φυλλομετρητή γίνονται γνωστά στους διαχειριστές των κοινωνικών δικτύων. Αυτές οι επιπλέον πληροφορίες, πιθανόν να μοιραστούν με τρίτους με στόχο να προσφέρουν σχετικές υπηρεσίες και διαφημίσεις στους χρήστες. Ένα ακόμη ερώτημα, που απασχολεί πολλούς χρήστες και μη των κοινωνικών δικτύων είναι, εάν κάποιος ο οποίος δεν είναι μέλος σε κάποιες απο αυτές τις ιστοσελίδες μπορεί να επισημανθεί στις φωτογραφίες οποιουδήποτε χρήστη. Η απάντηση είναι πως, ένας χρήστης έχει την δυνατότητα να επισημάνει οποιονδήποτε επιθυμεί. Ακόμη και αν το όνομα που πληκτρολογεί δεν υπάρχει στην λίστα των φίλων του, έχει την δυνατότητα να τοποθετήσει την ηλεκτρονική του διεύθυνση. Έτσι λοιπόν, ο δεύτερος θα λάβει ένα ηλεκτρονικό μήνυμα πως έχει επισημανθεί στη φωτογραφία κάποιου χρήστη - μέλους του δικτύου αυτού και αυτός με την σειρά του αποκτά πρόσβαση μόνο στην φωτογραφία, στην οποία είναι επισημασμένος και σε καμία άλλη πληροφορία απο το προφίλ του χρήστη, εκτός βέβαια και αν δημιουργήσει και αυτός λογαριασμό στο εν λόγω δίκτυο. Μία ακόμη πιθανή παραβίαση της ιδιωτικότητας των χρηστών μπορεί να συμβεί κατά την διάρκεια όπου ένας χρήστης σβήνει δεδομένα και προσωπικές του πληροφορίες απο το προφίλ. Για να γίνουμε πιο συγκεκριμένοι, κάποια στιγμή κάποιος χρήστης επιθυμεί και διαγράφει κάποια δεδομένα απο τον λογαριασμό του, τα δεδομένα αυτά όμως δεν διαγράφονται ταυτόχρονα και απο τις βάσεις δεδομένων της ιστοσελίδας του κοινωνικού δικτύου. Αυτό συμβαίνει, διότι σύμφωνα με τους διαχειριστές τα δεδομένα και οι πληροφορίες των χρηστών κρατούνται για κάποιο χρονικό διάστημα ακόμη και αν αυτά διαγραφούν απο το προφίλ, ώστε να υπάρχουν ως αντίγραφα ασφαλείας. Επιπλέον, παραβίαση της ιδιωτικότητας μπορεί να πραγματοποιηθεί κατά την αποδοχή ενός αιτήματος φιλίας το οποίο να είναι σπαμ

(=spam)[1] . Τα αιτήματα αυτά έχουν συνήθως την εξής μορφή, μία παραπλανητική φωτογραφία προφίλ και ένα συνοδευτικό κείμενο του τύπου "Γεια σε όλους, έχω δημιουργήσει εδώ ένα προφίλ, διότι στο προηγούμενο κοινωνικό δίκτυο που ήμουνα δεν μου επέτρεπαν να ανεβάζω φωτογραφίες με γυμνό υλικό. Εάν θέλετε να δείτε και άλλες περισσότερες φωτογραφίες μου, αποδεχτείτε το αίτημα φιλίας μου και πατήστε σε αυτόν τον σύνδεσμο. Δεν σας πάρει περισσότερο απο δύο λεπτά, αρκεί φυσικά να είστε άνω των 18 ετών". Η παραπάνω ενέργεια, η αποδοχή δηλαδή του αιτήματος φιλίας θα έχει ως αποτέλεσμα, ο χρήστης να πέσει θύμα απάτης και άτομα μη εξουσιοδοτημένα να αποκτήσουν πρόσβαση σε προσωπικές πληροφορίες του χρήστη και να στέλνουν στις επαφές του μηνύματα σπαμ. Ιδιαίτερη προσοχή πρέπει να δοθεί στα παραδείγματα παραβίασης της ιδιωτικότητας, τα οποία αναφέρονται στον Διαδικτυακό εκφοβισμό (Cyber-bullying)[2]. Περίπου, ένας στους δέκα νέους έχει μπλεχτεί σε καταστάσεις Διαδικτυακού εκφοβισμού, με ποσοστό 3,3% στο ρόλο του θύματος, 5% σε ρόλο δράστη και με το 2,6% να έχει βρεθεί στην θέση τόσο του θύματος, όσο και του δράστη. Επιπλέον, ένα άλλο συμβάν που μπορεί να θεωρηθεί ως παραβίαση της ιδιωτικότητας του χρήστη είναι, ότι το πραγματικό όνομα του χρήστη, του διαδικτυακό του όνομα και η φωτογραφία προφίλ του εμφανίζονται σε μηχανές αναζήτησης. Η αντιστοίχηση αυτή, ονόματος και φωτογραφίας μπορεί να αποβεί ιδιαίτερα επικίνδυνη, αφού οποιοσδήποτε σε οποιοδήποτε μέρος του κόσμου μπορεί να βλέπει το πραγματικό όνομα, αλλά και πρόσωπο του χρήστη. Ιδιαίτερο ενδιαφέρον, προκάλεσε το γεγονός, ότι σε γνωστό πανεπιστήμιο του εξωτερικού απορρίφθηκε αίτηση υποψηφίου, εξαιτίας συγκεκριμένου περιεχομένου που υπήρχε στο προσωπικό του προφίλ σε μία ιστοσελίδα κοινωνικής δικτύωσης. Είναι πλέον γεγονός, ότι πολλά κολλέγια και πανεπιστήμια του εξωτερικού, προτού κάνουν δεκτές τις αιτήσεις των υποψηφίων, ερευνούν τις πληροφορίες και τα δεδομένα που έχουν δημοσιοποιήσει στα διάφορα κοινωνικά δίκτυα. Στις Η.Π.Α. έχει δημιουργηθεί μεγάλο θέμα, καθώς τέτοιες ενέργειες υποδεικνύουν παραβίαση της ιδιωτικότητας των υποψηφίων και είναι ικανά να τους στερήσουν ακόμη και την φοίτηση στα εκπαιδευτικά ιδρύματα. Βέβαια, τα πανεπιστήμια απο την μεριά τους αποκλείουν

[1] **Σπαμ** (spam) ονομάζεται η μαζική αποστολή ηλεκτρονικών μηνυμάτων ή άλλων, σε μια προσπάθεια προώθησης προϊόντων ή ιδεών. Λόγω του χαμηλού κόστους αποστολής, η αποστολή γίνεται σε μεγάλο αριθμό αποδεκτών. Πρόκειται για παγκόσμιο φαινόμενο και υπάρχουν εκτιμήσεις για επτά τρισεκατομμύρια ανεπιθύμητα μηνύματα spam στο 2011. Σε αρκετές χώρες η αποστολή σπαμ διώκεται δικαστικά.

[2] Αφορά τον εκφοβισμό, την απειλή, την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων που δέχονται μέσω της χρήσης του Διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από ομηλίκους τους

όλες αυτές τις κατηγορίες, όμως το θέμα δεν έχει λήξει ακόμη. Κλείνοντας, καλό θα ήταν να αναφέρουμε, πόσο προσεχτικοί θα πρέπει να είναι οι χρήστες, όταν ανεβάζουν προσωπικές τους φωτογραφίες και ειδικά όσες περιέχουν καθαρή εικόνα του προσώπου τους. Πολλές φορές, οι εικόνες μπορεί να περιέχουν δεδομένα και πληροφορίες που να αποκαλύπτουν πολλά προσωπικά στοιχεία, όπως πρόσωπα της οικογένειας, την κατοικία διαμονής, μέρη που συχνάζει ο χρήστης, φίλους κλπ. Όλα τα προηγούμενα αποτελούν αυστηρά προσωπικά στοιχεία και μπορεί κάποιος που ούτε καν γνωρίζει ο χρήστης να τα χρησιμοποιήσει εναντίον του.

2.3 Παραδείγματα προστασίας της ιδιωτικότητας

Όπως αναφέρθηκε και παραπάνω, η αξία της προστασίας της ιδιωτικότητας είναι πολύ μεγάλη και μπορεί να γίνει ακόμη μεγαλύτερη, αν σκεφτεί κανείς πόσο εύκολα μπορεί να παραβιαστεί. Επομένως, χρήσιμο θα ήταν να παραθέσουμε κάποια παραδείγματα προστασίας της ιδιωτικότητας. Πρώτα απο όλα, αποτελεσματικό θα ήταν εάν οι χρήστες δεν δημοσίευαν φωτογραφίες, οι οποίες αποκαλύπτουν προσωπικά και ιδιωτικά δεδομένα. Ακόμη και αν επιθυμούν να ανεβάσουν φωτογραφικό υλικό, τότε καλό θα ήταν να προσέχουν σε ποιούς απο τους χρήστες του ίδιου κοινωνικού δικτύου θα δίνουν πρόσβαση. Επίσης, αποδοτικό θα ήταν, εάν οι γονείς των παιδιών, τα οποία έχουν λογαριασμό σε κάποιο κοινωνικό δίκτυο, να είναι ενήμεροι για τις πληροφορίες αλλά και τις φωτογραφίες που κοινοποιούν στις ιστοσελίδες αυτές. Έτσι, εάν παρατηρήσουν ότι τα παιδιά τους προβάλλουν ακατάλληλο περιεχόμενο να τα αποτρέψουν, καθώς επίσης και να τα συμβουλέψουν για τις συνέπειες που μπορεί να προκαλέσει η απροκάλυπτη έκθεση δεδομένων και φωτογραφιών. Επιπρόσθετα, τόσο οι έφηβοι όσο και οι ενήλικοι που είναι μέλη στις ιστοσελίδες κοινωνικής δικτύωσης, θα πρέπει να είναι ιδιαίτερα υποψιασμένοι και προσεχτικοί και να μην δέχονται εύκολα να συναντήσουν άτομα, τα οποία δεν γνωρίζουν και δεν έχουν δει ποτέ, απο κοντά, ξανά στην ζωή τους. Επιπλέον, ένας ακόμη τρόπος, ώστε να ενδυναμώσει κάποιος χρήστης την προστασία της ιδιωτικότητάς του, θα ήταν να μην ανοίγει και να μην διαβάζει μηνύματα, τα οποία φτάνουν σε αυτόν απο άγνωστους αποστολείς. Ακόμη, μηνύματα με ύποπτο περιεχόμενο, καλό θα ήταν να μην διαγράφονται, αλλά και να αναφέρονται σε

ειδικούς και αρχές που είναι υπεύθυνοι για την προστασία της ιδιωτικότητας των χρηστών του διαδικτύου και ειδικότερα των κοινωνικών δικτύων. Τέλος, στις μέρες μας, αποτελεί πλέον αναγκαιότητα οι χρήστες τόσο του διαδικτύου, όσο και των κοινωνικών δικτύων να ενημερώνονται και να είναι προσεχτικοί με τις πληροφορίες που δημοσιοποιούν, καθώς η παραβίαση της ιδιωτικότητας αποτελεί πλέον καθημερινότητα και οι συνέπειες της μπορεί να αποβούν μοιραίες και καταστροφικές.

Κεφάλαιο 3: Απειλές κατά της Ιδιωτικότητας στα Κοινωνικά Δίκτυα

3.1 Αποθήκευση και μελέτη προφίλ από τρίτους (Digital Dossier Aggregation)

3.1.1 Ορισμός κινδύνων

Τα διάφορα προφίλ των χρηστών που δημιουργούνται και υπάρχουν στα κοινωνικά δίκτυα, μπορούν εύκολα να προσβληθούν από τρίτους και κυρίως μη εξουσιοδοτημένους χρήστες. Η μελέτη και η μαζική αποθήκευση προσωπικών δεδομένων από "αγνώστους" μπορεί να προκαλέσει μία ποικιλία προβλημάτων, καθώς πολλές φορές χρησιμοποιούνται για σκοπούς που ο ίδιος ο χρήστης ποτέ δεν υπολόγισε. Τα προσωπικά προφίλ του καθενός, συνήθως, περιέχουν πληροφορίες, οι οποίες εύκολα μπορούν να αποκαλυφθούν σε τρίτους τόσο απροκάλυπτα όσο και συγκαλυμμένα, με αποτέλεσμα ευαίσθητα προσωπικά δεδομένα να γνωστοποιούνται. Ένα απλό παράδειγμα είναι η συλλογή των τοποθεσιών, που έχει επισημανθεί ενίοτε ο χρήστης. Επιπλέον, μία πιο συχνή και ίδιας σημασίας απειλή αποτελεί η αποκάλυψη ονόματος, επιθέτου ακόμα και φωτογραφίας από μία απλή αναζήτηση σε ένα κοινωνικό δίκτυο. Κάπου εδώ θα ήταν χρήσιμο, να αναλύσουμε την αξία των προσωπικών πληροφοριών και δεδομένων του χρήστη έξω από τα όρια του εκάστοτε κοινωνικού δικτύου. Τι γίνεται λοιπόν, όταν οι πληροφορίες αυτές δρουν εκτός του περιβάλλοντος του κοινωνικού δικτύου και πόσο "καταστροφικές" μπορούν να αποδειχτούν για έναν χρήστη οποιοδήποτε τέτοιου δικτύου; Δυστυχώς, ακόμη και εάν ο χρήστης αλλάξει ή έστω διαγράψει κάποια δεδομένα από το προσωπικό του προφίλ, αυτά υπάρχουν αποθηκευμένα και καταχωρημένα κάπου "αλλού", όπου και θα γίνει εκτενέστερη ανάλυση παρακάτω. Έτσι, τα ήδη καταγεγραμμένα προσωπικά δεδομένα κάποιου έχουν την ικανότητα να στραφούν εναντίον του και να γίνουν πολύ επικίνδυνα για τον ίδιο. Για να γίνει πιο κατανοητό το παραπάνω, αποτελεσματικό θα ήταν να δώσουμε μερικά παραδείγματα. Παλαιότερα, είχε δημιουργηθεί μεγάλο

σκάνδαλο γύρω από το όνομα γνωστού μοντέλου, όπου είχε λάβει μέρος σε διαγωνισμό ομορφιάς, ήρθε πρώτη αλλά λίγο αργότερα της ζητήθηκε να επιστρέψει πίσω το στέμμα, εξαιτίας φωτογραφικού πορνογραφικού υλικού που βρέθηκε αναρτημένο στο προσωπικό της προφίλ σε γνωστό κοινωνικό δίκτυο. Επιπλέον, ένα ακόμη εξίσου αξιοσημείωτο παράδειγμα είναι αυτό, όπου υπάλληλοι γνωστής εταιρίας κατηγορούσαν τον εργοδότη τους στα προφίλ κοινωνικού δικτύου, όπου και έκαναν χρήση, με αποτέλεσμα οι πληροφορίες αυτές να δημοσιοποιηθούν από τρίτους στον ίδιο τον εργοδότη και οι υπάλληλοι να χάσουν τις θέσεις εργασίας τους. Από τα παραδείγματα λοιπόν, γίνεται φανερό το πόσο σοβαρή απειλή κατά της ιδιωτικότητας μπορεί να εξελιχθεί η αποθήκευση και η μελέτη προφίλ από τρίτους.

3.1.2 Προτεινόμενες λύσεις ενάντια στη μελέτη και αποθήκευση προφίλ από τρίτους

Πρώτα από όλα, οι χρήστες των κοινωνικών δικτύων, θα ήταν χρήσιμο να ενημερώνονται πλήρως για τους διάφορους κινδύνους που εγκυμονούν κατά την χρήση οποιουδήποτε κοινωνικού δικτύου. Κατά καιρούς, έχει δημιουργηθεί μία πληθώρα από καμπάνιες και εκστρατείες, όπου σκοπό έχουν τόσο να ενημερώσουν, όσο και να προστατέψουν τους χρήστες από τις διάφορες κατατοπιές. Βέβαια, η κινητοποίηση αυτή των διαφόρων οργανώσεων δεν είναι ακόμη ιδιαίτερα διαδεδομένη και πραγματοποιούνται διάφορες ενέργειες, έτσι ώστε οι διάφοροι χρήστες να γνωρίζουν πλήρως, πως να κάνουν ορθή και ασφαλή χρήση των κοινωνικών δικτύων. Στόχος όλων αυτών είναι να δημιουργούν γραφικά περιβάλλοντα, τα οποία θα είναι φιλικά προς τους χρήστες, προσφέροντας με αυτόν τον τρόπο οδηγίες και συμβουλές που θα ενστερνιστούν ευκολότερα από τους τελευταίους. Πολλά από τα κοινωνικά δίκτυα έχουν ήδη ξεκινήσει να υιοθετούν διάφορες πολιτικές προστασίας προσωπικών δεδομένων. Χαρακτηριστικό παράδειγμα αποτελεί η απαγόρευση κοινοποίησης ταχυδρομικού κώδικα των χρηστών, καθώς επίσης αποτελεσματικό θα ήταν οι χρήστες εκτός από το παραπάνω στοιχείο να υποκρύπτουν και άλλα από τα προσωπικά τους στοιχεία, όπως η διεύθυνση κατοικίας τους, ο αριθμός του κινητού τους τηλεφώνου κλπ. Επιπλέον,

ιδιαίτερα χρήσιμο θα ήταν εάν όλες οι καμπάνιες και οι εκστρατείες αυτές ερχόντουσαν σε επαφή με τους ίδιους τους προγραμματιστές και τους κατασκευαστές των κοινωνικών δικτύων, ενημερώνοντας τους για την δράση τους. Αυτό όμως αποτελεί έργο δύσκολο, καθώς οι εταιρείες των διαφόρων κοινωνικών δικτύων μπροστά στην διάδοση του δικτύου τους και τον βωμό του κέρδους αγνοούν οτιδήποτε μπορεί να τους σταθεί "εμπόδιο" ! Επιπλέον, τα κοινωνικά δίκτυα θα ήταν αποδοτικό, να συμβαδίζουν με τις ισχύουσες νομοθεσίες των χωρών, στις οποίες πραγματοποιείται εκτεταμένη χρήση τους. Από την άλλη πλευρά, τόσο στην Ελλάδα όσο και στην υπόλοιπη Ευρώπη, οι ισχύουσες νομοθεσίες δεν ανταποκρίνονται πλήρως στους κινδύνους που υπάρχουν σήμερα γύρω από τα κοινωνικά δίκτυα και την προστασία από την μελέτη και αποθήκευση προφίλ από τρίτους. Ακόμη, η υιοθέτηση και η προώθηση πιστοποίησης - αυθεντικοποίησης των χρηστών στα διάφορα περιβάλλοντα των κοινωνικών δικτύων μπορεί να συντελέσει στην βέλτιστη προστασία των χρηστών, από την απειλή κάποιου τρίτου να προσποιηθεί έναν οποιοδήποτε χρήστη, συλλέγοντας έτσι πληροφορίες για τις οποίες δεν είναι εξουσιοδοτημένος. Οι χρήστες όμως είναι ακόμη δύσπιστοι ως προς το να χρησιμοποιήσουν στοιχεία, που θα ήταν ικανά να πιστοποιήσουν την ταυτότητα τους, όπως για παράδειγμα η αποκάλυψη αριθμού κινητού τηλεφώνου ή ακόμη και η δήλωση κάποιου συγκεκριμένου προσωπικού αριθμού, ο οποίος θα είναι αναγνωρισμένος από το ίδιο το κράτος (π.χ. ΑΦΜ [αριθμός φορολογικού μητρώου], ΑΔΤ [αριθμός δελτίου ταυτότητας]) . Παρόλα αυτά, μερικά κοινωνικά δίκτυα, όπως το LinkedIn, ήδη χρησιμοποιούν μηχανισμούς αυθεντικοποίησης των χρηστών και προσπαθούν όσο αυτό είναι δυνατόν, να χρησιμοποιούν φιλικούς προς τους χρήστες μηχανισμούς, δημιουργώντας τους έτσι μία αίσθηση εμπιστοσύνης και ασφάλειας. Επίσης, ιδιαίτερα αποτελεσματικό θα ήταν, οι παροχείς των διαφόρων κοινωνικών δικτύων να συμφωνούσαν με τους διάφορους διαχειριστές των μηχανών αναζήτησης, έτσι ώστε τα διάφορα δεδομένα των χρηστών να μην αποκαλύπτονται σε πιθανές αναζητήσεις στις μηχανές αυτές. Για να γίνουμε πιο συγκεκριμένοι, δεδομένα αλλά και πληροφορίες χρηστών κοινωνικών δικτύων, όπως για παράδειγμα ονοματεπώνυμο, φωτογραφίες, διευθύνσεις, λογαριασμός ηλεκτρονικού ταχυδρομείου κλπ, θα πρέπει να παραμένουν ιδιωτικά και να μην γνωστοποιούνται μέσα από τις διάφορες μηχανές αναζήτησης ή έστω και αν δημοσιοποιούνται, ο χρήστης να έχει την δυνατότητα να τα αποσύρει και να τα διαγράψει, εάν και εφόσον το επιθυμεί.

3.2 Δευτερεύουσα Αποθήκευση Πληροφοριών (Secondary Data Collection)

3.2.1 Ανάλυση βασικών κινδύνων

Ως γνωστόν, τα μέλη των κοινωνικών δικτύων αποκαλύπτουν διάφορα προσωπικά τους δεδομένα, αλλά και στοιχεία της προσωπικότητάς τους. Πέραν όμως από τις πληροφορίες που ίδιοι δημοσιεύουν, στην ουσία αποκαλύπτουν και μία πληθώρα πληροφοριών χρησιμοποιώντας το δίκτυο αυτό καθ' εαυτό. Πιο αναλυτικά, όταν κάποιος χρήστης συνδέεται σε κάποιο κοινωνικό δίκτυο, τότε αυτόματα αποκαλύπτονται στους διαχειριστές των δικτύων στοιχεία όπως η διάρκεια παραμονής στο συγκεκριμένο δίκτυο, η διεύθυνση σύνδεσης (= IP address), το ιστορικό επισκέψεων προφίλ άλλων χρηστών, ακόμη και μηνύματα, όπου ο χρήστης είτε στέλνει είτε λαμβάνει. Στα παραπάνω προβλήματα έρχεται να προστεθεί και το εξής, καθώς οι χρήστες συνδέονται τόσο από διαφορετικά σημεία (π.χ. σπίτι, χώρος εργασίας, χώρος διασκέδασης), όσο και από διαφορετικές συσκευές και μέσα (π.χ. ηλεκτρονικός υπολογιστής, κινητό, ταμπλέτα) οδήγησαν τους διαχειριστές των κοινωνικών δικτύων να συγκεντρώνουν όλα τα δεδομένα των χρηστών κάτω από έναν ενιαίο παροχέα (= provider). Αυτό, δυστυχώς, παρέχει την δυνατότητα στους ιδιοκτήτες των κοινωνικών δικτύων, να διατηρούν μεγάλες "αποθήκες" δεδομένων και προσωπικών πληροφοριών των χρηστών κάτω από τον έλεγχό τους. Επιπλέον, ιδιαίτερη ανησυχία έχει προκαλέσει το γεγονός, όπου μέσα στην πολιτική προστασίας που ακολουθούν τα δίκτυα αυτά υπάρχουν ασάφειες που δεν προσφέρουν μία πλήρη και αντικειμενική εικόνα στους χρήστες, σχετικά με την διαφύλαξη των προσωπικών τους πληροφοριών. Για να γίνουμε πιο συγκεκριμένοι, οι δηλώσεις των κοινωνικών δικτύων περί ιδιωτικότητας υπογραμμίζουν, πως έχουν πρόσβαση στα δεδομένα των χρηστών και μπορούν αφενός να τα χρησιμοποιούν με σκοπό να βελτιώσουν τις υπηρεσίες που παρέχουν, αφετέρου να τις αποκαλύψουν και να τις πουλήσουν σε τρίτους, οι οποίοι από την μεριά τους στοχεύουν σε επικερδείς προωθήσεις προϊόντων, διαφημίσεις και σχετικές υπηρεσίες. Έτσι, ο κίνδυνος που παραμονεύει από την συλλογή δευτερευόντων πληροφοριών και δεδομένων είναι ύψιστης

σημασίας. Καθώς η διάδοση των κοινωνικών μέσων είναι ραγδαία και όλο και περισσότεροι χρήστες του διαδικτύου γίνονται μέλη σε αυτά, η αποκάλυψη των προσωπικών τους δεδομένων σε τρίτους, οι οποίοι συλλέγουν τα στοιχεία που τους ενδιαφέρουν και τα εκμεταλλεύονται ανάλογα, είτε για να τα μεταπωλήσουν είτε για να διαφημίσουν προϊόντα και υπηρεσίες, είναι ιδιαίτερα ανησυχητική! Τα κέρδη των εταιρειών των κοινωνικών δικτύων από τα παραπάνω είναι τεράστια. Αξίζει να αναφερθεί, πως το 2006 η εταιρεία MySpace πουλούσε πληροφορίες με το αντίτιμο των 35 δολαρίων ανά χρήστη και πως στο τέλος του Δεκεμβρίου του 2011, οι ενεργοί χρήστες μηνιαίως στο Facebook κατάφεραν να αγγίξουν τον αριθμό των 845 εκατομμυρίων. Επομένως, είναι εύκολο να φανταστούμε για τον όγκο των οικονομικών ποσών που διακινούνται σε αυτές τις επιχειρήσεις.

3.2.2 Προτάσεις για την βέλτιστη προστασία των χρηστών

Η προστασία των χρηστών από την διαρροή προσωπικών τους δεδομένων και πληροφοριών άρχισε να μετατρέπεται σιγά σιγά σε μία επιτακτική ανάγκη. Έτσι, οι ειδικοί επί της προστασίας προσωπικών δεδομένων ξεκίνησαν να ασχολούνται με την εύρεση τρόπων, όπου οι χρήστες θα μπορούν από την μεριά τους να διαφυλάσσονται όσο το δυνατόν καλύτερα. Πολλοί από τους χρήστες των κοινωνικών δικτύων ξεκίνησαν να αλλάζουν τις προκαθορισμένες ρυθμίσεις (default settings), που υπάρχουν στα δίκτυα αυτά, με στόχο τον καλύτερο έλεγχο του προφίλ τους και των πληροφοριών που δημοσιεύουν. Αναλυτικότερα, οι χρήστες έχουν την δυνατότητα να αλλάζουν τις ρυθμίσεις αυτές σύμφωνα με τις προσωπικές τους επιθυμίες. Για παράδειγμα, μπορούν να επιλέξουν ποιοί από τους χρήστες του ίδιου κοινωνικού δικτύου θα έχουν πρόσβαση στις διάφορες πληροφορίες που δημοσιοποιούν. Στα διάφορα δεδομένα λοιπόν, μπορούν να έχουν πρόσβαση μόνο οι φίλοι του χρήστη ή μόνο η οικογένεια ή μόνο συγκεκριμένα άτομα που ο χρήστης επιθυμεί κλπ. Οι προκαθορισμένες ρυθμίσεις ωστόσο αναφέρονται και σε άλλα ζητήματα, όχι μόνο στις δημοσιοποιημένες πληροφορίες. Πιο συγκεκριμένα, με τις ρυθμίσεις αυτές, ο χρήστης είναι ικανός να δημιουργήσει ένα πιο ασφαλές περιβάλλον δράσης κατά την πλοήγησή του στο δίκτυο. Μερικά παραδείγματα είναι ότι μπορεί να καθορίσει ποιοί

από τους χρήστες μπορούν να του στέλνουν προσωπικά μηνύματα ή ποιοί από τους χρήστες θα έχουν πρόσβαση στις φωτογραφίες του ή ακόμη και να ελέγχεται κάθε φορά η διεύθυνση σύνδεσης του χρήστη και αν δεν είναι η συνηθισμένη να ζητείται κάποιου είδους ταυτοποίηση. Οι προδιαγεγραμμένες ρυθμίσεις ωστόσο, θα ήταν απότελεσματικό εάν διέθεταν και κάποιο τρόπο ελέγχου της ηλικίας του χρήστη που πρόκειται να συνδεθεί στο εν λόγω δίκτυο και να τοποθετούσαν σαν όριο ηλικίας τα 21 χρόνια και πάνω. Το πιο σημαντικό όμως όλων είναι τα κοινωνικά δίκτυα να προάγουν ένα σύνολο από οδηγίες, οι οποίες θα ενισχύουν το ενδιαφέρον των χρηστών, ώστε να τροποποιούν τις διάφορες ρυθμίσεις των λογαριασμών τους, απόκτώντας έτσι τον καλύτερο δυνατό έλεγχο των δεδομένων τους αλλά και την προστασία της ιδιωτικότητάς τους. Επιπλέον, απόδοτικό θα ήταν, το περιβάλλον των ρυθμίσεων να παρουσιάζεται φιλικό προς τους χρήστες και οι οδηγίες να εξηγούνται με απλές και κατανοητές λέξεις, προτρέποντάς τους έτσι να τις διαμορφώσουν όπως οι ίδιοι επιθυμούν. Ενάντια τώρα στην απειλή της δευτερεύουσας αποθήκευσης πληροφοριών, έρχεται κάτι νέο για τα μέχρι υπάρχοντα δεδομένα, γνωστή και ως φορητότητα των δικτύων (Portable Social Networks). Με τον όρο αυτό, αναφερόμαστε στην δυνατότητα, που θα μπορεί να έχει ο χρήστης ενός συγκεκριμένου κοινωνικού δικτύου να μεταφέρει, τόσο δεδομένα και πληροφορίες, όσο και ρυθμίσεις λογαριασμού και απόρρήτου. Πιο αναλυτικά, τα κοινωνικά δίκτυα καλό θα ήταν να απόκτήσουν αυτές τις τεχνικές φορητότητας, έτσι ώστε όταν κάποιος χρήστης επιθυμεί να γίνει μέλος σε ένα καινούργιο δίκτυο να έχει την επιλογή αυτή. Κάτι τέτοιο αποτελεί μεγάλη καινοτομία, καθώς ο χρήστης δεν είναι αναγκαίο να σπαταλήσει χρόνο και κόπο για να γίνει μέλος σε μια νέα ιστοσελίδα κοινωνικής δικτύωσης. Έτσι, ο χρήστης δεν θα χρειάζεται να ξαναπληκτρολογήσει όνομα, κωδικό, διευθυνση ηλεκτρονικού ταχυδρομείου, ούτε φυσικά και να ψάξει να βρει τους φίλους του, οι οποίοι είναι επίσης μέλη στο συγκεκριμένο δίκτυο και ούτε να ρυθμίσει ξανά το ποιοί και τι πρόσβαση θα έχουν στις προσωπικές του πληροφορίες. Βέβαια, οποιδήποτε τέτοια ενέργεια κρύβει από πίσω της οικονομικούς αλλά και εμπορικούς σκοπούς, όμως δεν θα πρέπει να παραλείπεται η ασφάλεια και η προστασία των ίδιων των χρηστών και των δεδομένων τους. Δυστυχώς, η υιοθέτηση της φορητότητας από τα κοινωνικά δίκτυα δεν είναι ιδιαίτερα διαδεδομένη, ελπίζουμε όμως με την εξέλιξη της τεχνολογίας των ηλεκτρονικών υπολογιστών και δικτύων και ό,τι άλλο συνοδεύει την εξέλιξη αυτή, η οποία είναι αναμφισβήτητα ραγδαία, να επιτευχθεί και αυτός ο στόχος. Όπως έχουμε ήδη αναφέρει, η βέλτιστη προστασία

των χρηστών, από την δευτερεύουσα αποθήκευση πληροφοριών κατά την πλοήγησή τους στα κοινωνικά δίκτυα αποτελεί αντικείμενο αυτής της ενότητας. Η προσπάθεια αυτήν λοιπόν, μπορεί να εμπλουτιστεί, εάν αναλυθεί περισσότερο η "διαφάνεια" του τρόπου με τον οποίο συλλέγονται και επεξεργάζονται τα δεδομένα των χρηστών από τρίτους. Για να γίνουμε πιο συγκεκριμένοι, υπάρχουν καίρια ερωτήματα που ακόμη μένουν αναπάντητα. Μερικά από αυτά είναι όπως, ποιός είναι ο σκοπός της συλλογής δεδομένων και ληροφοριών από τρίτους, ποιοί τελικά είναι ακριβώς αυτοί που μπορούν να απόκτούν πρόσβαση στις διάφορες πληροφορίες, όπως επίσης εάν υπάρχει κάποιος συγκεκριμένος τρόπος πρόσβασης και αλλαγής των δεδομένων αυτών. Πολύ σημαντικό, είναι όλοι οι χρήστες να μπορούν να έχουν μία πλήρη εικόνα του τι πραγματικά συμβαίνει με τα προσωπικά τους δεδομένα, πριν αλλά και μετά την σύνδεση τους στον προσωπικό τους λογαριασμό. Αυτή η πλήρης και αντικειμενική εικόνα, καλό θα ήταν, να εκφράζεται μέσα από ένα φιλικό προς τον χρήστη τρόπο, βοηθώντας τον έτσι να γνωρίζει όσα περισσότερα γίνεται και όχι να τον "απόμακρύνει" κάνοντας χρήση αυστηρών κανόνων και οδηγιών.

3.3 Αναγνώριση Φυσικών Προσώπων (Face Recognition)

3.3.1 Απειλές και βασικοί κίνδυνοι

Ένα από τα πιο διαδεδομένα φαινόμενα της εποχής αποτελεί η συμμετοχή των χρηστών στα διάφορα κοινωνικά δίκτυα. Η συμμετοχή αυτή, συχνά συνοδεύεται από την τάση των χρηστών να δημοσιεύουν πληθώρα φωτογραφιών, τόσο με τους ίδιους, όσο και με τους φίλους σε ποικίλες προσωπικές στιγμές. Ιδιαίτερη έκπληξη προκάλεσε η δημοσίευση μερικών στατιστικών στοιχείων, από την εταιρεία Facebook, τον Μάιο του 2007. Το γεγονός αυτό συνέβη, διότι τα νούμερα τα οποία παρουσιάστηκαν, ξεπέρασαν κάθε προσδοκία. Πιο συγκεκριμένα, μέχρι τον Μάιο του

2007, η εταιρεία είχε στην κατοχή της ένα κόμμα εφτά δισεκατομμύρια (= 1.700.000.000) προσωπικές φωτογραφίες χρηστών και δύο κόμμα δύο δισεκατομμύρια (= 2.200.000.000) χρήστες είχαν επισημανθεί σε φωτογραφίες άλλων φίλων τους. Τα τεράστια αυτά νούμερα ήρθαν για να επιβεβαιώσουν, αφενός την διάδοση των κοινωνικών δικτύων, αφετέρου τον απίστευτα μεγάλο αριθμό αποθηκευμένου φωτογραφικού υλικού, όπου διαθέτει η συγκεκριμένη εταιρεία. Επιπλέον, η εταιρεία από την μεριά της διαθέτει πολύ μεγάλους χώρους αποθήκευσης δεδομένων, αφού οι χρήστες καταφέρνουν να ξεπερνάνε τον αριθμό των εξήντα εκατομμυρίων (= 60.000.000) φωτογραφιών που δημοσιεύουν την εβδομάδα. Η τάση, λοιπόν αυτή, προήλθε από το γεγονός ότι κατά την δημιουργία λογαριασμού και προφίλ στα συγκεκριμένα κοινωνικά δίκτυα, πέρα από την καταγραφή προσωπικών πληροφοριών και δεδομένων, ο χρήστης δημοσίευε και μία προσωπική του φωτογραφία προφίλ, έτσι ώστε οι μελλοντικοί του φίλοι που θα τον αναζητήσουν μέσα στο όποιο δίκτυο, να είναι σε θέση να επιβεβαιώσουν την ταυτότητά του. Βέβαια, την ίδια στιγμή όπου οι φωτογραφίες των χρηστών αυξάνονται με τους ρυθμούς που προαναφέραμε, ταυτόχρονα δημιουργούνται και αλγόριθμοι αναγνώρισης προσώπων. Με το πέρασμα του χρόνου, οι αλγόριθμοι αυτοί γίνονται όλο και ταχύτεροι, αλλά και πιο αποδοτικοί. Ο συνδυασμός γρήγορου υπολογιστικού υλικού με όλο και καλύτερους αλγόριθμους αναγνώρισης προσώπων κατάφερε την σύγκριση μεγάλου αριθμού φωτογραφιών ταυτόχρονα. Έτσι, ο κίνδυνος αναγνώρισης κάποιου προσώπου, ακόμη και εάν αυτός χρησιμοποιεί ψευδώνυμο και ψεύτικες πληροφορίες είναι εύκολο να αποκαλυφθεί. Επίσης, είναι πολύ εύκολο τρίτοι και κυρίως μη εξουσιοδοτημένοι χρήστες να συλλέξουν πληροφορίες, αλλά και φωτογραφίες ενός χρήστη και να τις χρησιμοποιήσουν εναντίον του. Ακόμη, μέσα από την συλλογή προσωπικών φωτογραφιών είναι πολύ εύκολο να αποκαλυφθούν περαιτέρω πληροφορίες, που ο χρήστης πιθανόν να επιθυμεί να αποκρύψει και να μην γνωρίζει πως με την δημοσίευσή τους θα οδηγηθεί σε τέτοιες δυσάρεστες καταστάσεις. Δυστυχώς, η αναγνώριση προσώπων αποτελεί μία από τις σημαντικότερες απειλές κατά της ιδιωτικότητας, καθώς είναι πιθανό να αποκαλυφθούν σημαντικά προσωπικά δεδομένα. Αυτά είναι αρκετά δύσκολο να προστατευτούν νομικά, καθώς οι ισχύουσες νομοθεσίες δεν περιλαμβάνουν διατάξεις που να αφορούν την προστασία των χρηστών από την αποκάλυψη των φυσικών τους προσώπων μέσα από τα κοινωνικά δίκτυα. Τελευταίο, όμως εξίσου σημαντικό είναι το παράδειγμα, όπου μπορεί να πραγματοποιηθεί και να αποκαλυφθεί η σύνδεση

μεταξύ ενός ψεύτικου προφίλ σε δίκτυο γνωριμιών και ενός πραγματικού προφίλ σε οποιοδήποτε άλλο δίκτυο.

3.3.2 Μέτρα προστασίας ενάντια στην αποκάλυψη προσώπων

Ιδιαίτερη προσοχή θα πρέπει να δοθεί, όσο αναφορά την αντιμετώπιση της σημαντικής αυτής απειλής κατά της ιδιωτικότητας, που αναφέρεται βεβαίως στην αποκάλυψη των φυσικών προσώπων των χρηστών. Η σωστή ενημέρωση, αλλά και εκπαίδευση των χρηστών σχετικά με τους κινδύνους, που μπορεί να κρύβονται πίσω από τη δημοσίευση οποιουδήποτε φωτογραφικού υλικού, είτε από τους ίδιους, είτε ακόμη και από τους φίλους τους, αποτελεί την πηγή των μέτρων προστασίας. Συχνό είναι το φαινόμενο, όπου οι χρήστες μετατρέπονται σε θύματα απάτης και κλοπής προσωπικών τους δεδομένων, εξαιτίας της άγνοιάς τους περί προστασίας. Ωστόσο, κατά καιρούς έχουν δημιουργηθεί ποικίλες οργανώσεις που στόχο έχουν να ενημερώνουν τον κόσμο για τους κινδύνους που κρύβονται κατά την πλοήγησή τους στο διαδίκτυο, καθώς επίσης και για τις απειλές που ενδέχεται να παρουσιαστούν από τη δημοσίευση φωτογραφικού υλικού από διάφορες προσωπικές τους στιγμές. Άλλωστε είναι φανερό, πως οι δημοσιευμένες φωτογραφίες των χρηστών μπορεί να περιέχουν πληροφορίες, οι οποίες αποκαλύπτουν την τοποθεσία που βρίσκεται κάποιος ή ακόμη και την ταυτοποίηση ενός προσώπου. Επιπλέον, οι φωτογραφίες είναι πιθανό να αποκαλύπτουν προσωπικά δεδομένα άλλων ανθρώπων, όταν κυρίως επισημαίνονται με την χρήση μεταδεδομένων (= metadata). Την ίδια στιγμή, στις περισσότερες χώρες, τόσο τα σχολεία όσο και οι ίδιοι οι εκπαιδευτικοί έχουν αναλάβει το έργο της σωστής ενημέρωσης σε γονείς, αλλά και μαθητές ταυτόχρονα. Η συμμετοχή ανηλίκων στα διάφορα κοινωνικά δίκτυα αποτελεί τάση της εποχής και οι γονείς τους καλό θα ήταν, να ελέγχουν τις φωτογραφίες τις οποίες ανεβάζουν στις ιστοσελίδες αυτές κοινωνικής δικτύωσης. Η παραπάνω ενέργεια θα βοηθήσει τους γονείς να αποτρέψουν τον κίνδυνο, τα παιδιά τους να προβάλλουν πληροφορίες που δεν είναι αναγκαίο, όπως για παράδειγμα ενδιαφέροντα, ασχολίες ακόμη και την τοποθεσία του ίδιου τους του σχολείου. Επίσης, ιδιαίτερη βαρύτητα πρέπει να δοθεί στις ισχύουσες νομοθετικές διατάξεις της κάθε χώρας, αφού ακόμη δεν έχουν

διευκρινιστεί πλήρως τα δικαιώματα περί προστασίας της ιδιωτικότητας κατά την συμμετοχή των χρηστών στα διάφορα κοινωνικά δίκτυα, κάτι το οποίο τα δίκτυα από την μεριά τους το χρησιμοποιούν προς όφελός τους. Δυστυχώς, είναι ακόμη άγνωστο το τι προβλέπει η νομοθεσία σχετικά με την επισήμανση προσώπων σε φωτογραφίες από τρίτους και όχι από τα ίδια τα φυσικά πρόσωπα. Αποτελεσματικό όμως, θα ήταν εάν τα μέλη των κοινωνικών δικτύων παραμετροποιούσαν οι ίδιοι τις προκαθορισμένες ρυθμίσεις, μειώνοντας έτσι τον κίνδυνο της αποκάλυψης του φυσικού τους προσώπου εάν και εφόσον δεν το επιθυμούν. Ένα τέτοιο παράδειγμα είναι, όπου ο χρήστης μπορεί να απαγορεύσει την επισήμανση του εαυτού του σε φωτογραφίες τρίτων ή εάν κάποιος επιθυμεί να τον επισημάνει, πριν από αυτήν την ενέργεια αυτή να ζητείται η συγκατάθεσή του.

3.4 Καταγραφή στοιχείων χρήστη μέσω φωτογραφιών (C.B.I.R - Content-based Image Retrieval)

3.4.1 Ορισμός και υποψήφιοι κίνδυνοι και απειλές

Η ανάκτηση στοιχείων μέσα από το περιεχόμενο μιας φωτογραφίας (=CBIR) αποτελεί μια εφαρμογή, η οποία είναι βασισμένη σε ένα σύνολο από μεθόδους που αποκτούν, επεξεργάζονται, αναλύουν και αντιλαμβάνονται εικόνες μέσα από ένα ψηφιακό σύνολο δεδομένων και παράγουν μία ποικιλία πληροφοριών. Για να γίνουμε πιο συγκεκριμένοι, η εφαρμογή αυτή εστιάζει κυρίως στα πραγματικά δεδομένα μιας φωτογραφίας, παρά στα μεταδεδομένα της (επισημάνσεις, λέξεις κλειδιά), όπως χρώματα, σχήματα, επιφάνειες κλπ. Οι εφαρμογές αυτές δημιουργήθηκαν κατά κύριο λόγο, για να χρησιμοποιηθούν ευρύτερα στον τομέα της εγκληματολογίας. Η ανάκτηση στοιχείων μέσα από το περιεχόμενο μιας φωτογραφίας (=CBIR) αποτελεί μια αναπτυσσόμενη τεχνολογία, η οποία συλλέγει και κατά κάποιο τρόπο ταιριάζει χαρακτηριστικά και ιδιότητες, καταλήγοντας έτσι στα αποτελέσματα που αναζητά.

Πρόσφατα, παρά τις διάφορες ρυθμίσεις περί ιδιωτικότητας, αλλά και τις οδηγίες που δόθηκαν στα κοινωνικά δίκτυα σχετικά με τις φωτογραφίες που δημοσιεύονται από τους χρήστες, οι τελευταίοι παρουσιάστηκαν ανενημέρωτοι. Αρκετά είναι τα παραδείγματα εκείνων, οι οποίοι έχουν πλήρη άγνοια της εφαρμογής αυτής και των συνεπειών που ίσως μπορεί να επιφέρει και συνεχίζουν να δημοσιοποιούν πλούσιο φωτογραφικό υλικό. Όπως υφίσταται η απειλή της αποκάλυψης και αναγνώρισης φυσικών προσώπων μέσα από τις φωτογραφίες, έτσι υπάρχει και η σύνδεση και η αποκάλυψη πληροφοριών σχετικές με δεδομένα τοποθεσιών και γεωγραφικών θέσεων. Πολλές φορές, μέσα από μία φωτογραφία μπορεί να αποκαλυφθεί ο χώρος διαμονής ενός χρήστη και έπειτα, εξαιτίας της πληροφορίας αυτής, ο χρήστης να μετατραπεί σε θύμα παρακολούθησης, εκβιασμού ή ακόμη και στόχος για ανεπιθύμητες διαφημίσεις προϊόντων και υπηρεσιών. Είναι φανερό λοιπόν, πως ο κίνδυνος από την δημοσίευση φωτογραφιών και την ανάκτηση πληροφοριών μέσα από αυτές είναι ιδιαίτερα μεγάλος και κρύβει διάφορες απειλές, τις οποίες οι περισσότεροι χρήστες δύσκολα θα σκεφτούν. Η ανάκτηση στοιχείων μέσα από το περιεχόμενο μιας φωτογραφίας (=CBIR) έχει αναπτυχθεί ιδιαίτερα στο χώρο των ηλεκτρονικών υπολογιστών τα τελευταία χρόνια και πολλοί αλγόριθμοι έχουν δημιουργηθεί με στόχο την ταχύτερη και αποτελεσματικότερη έρευνα γύρω από το συγκεκριμένο θέμα. Την τεχνολογία αυτή, την εκμεταλλεύονται τόσο υπηρεσίες σχετικές με την δικαιοσύνη, όσο και υπηρεσίες σχετικές με την διαφήμιση και την προώθηση προϊόντων. Οι ιστοσελίδες κοινωνικής δικτύωσης από την μεριά τους, εξαιτίας του τεράστιου όγκου δεδομένων που διαθέτουν από φωτογραφίες χρηστών, αποτελούν πηγή πλούσιου υλικού για τις εφαρμογές της συγκεκριμένης τεχνολογίας.

3.4.2 Πρακτικές για την αντιμετώπιση καταγραφής στοιχείων χρήστη μέσα από φωτογραφίες

Πρώτα από όλα, οι χρήστες των κοινωνικών δικτύων πρέπει να συνειδητοποιήσουν, πως μία φωτογραφία μπορεί να λειτουργήσει ως διασύνδεση μεταξύ των προφίλ στις διάφορες ιστοσελίδες κοινωνικής δικτύωσης, όπου ο συγκεκριμένος διατηρεί λογαριασμό. Καθώς λοιπόν, οι αλγόριθμοι, που έχουν εμφανιστεί κατά καιρούς και

στόχο έχουν την ανάκτηση πληθώρας πληροφοριών μέσα από μία εικόνα, είναι ακόμη υπό κατασκευή και σε ερευνητικό στάδιο, οι χρήστες από την μεριά τους μπορούν να λάβουν κάποια προληπτικά μέτρα. Πιο αναλυτικά, οι χρήστες μπορούν να περιορίσουν σε μεγάλο βαθμό τον κίνδυνο καταγραφής προσωπικών τους δεδομένων και στοιχείων από τρίτους. Αυτό μπορεί να επιτευχθεί, εάν αρχικά οι χρήστες δεν κοινοποιούν φωτογραφίες, στις οποίες φαίνονται καθαρά όλα τα χαρακτηριστικά του προσώπου τους. Επιπλέον, θα ήταν ιδιαίτερα αποτελεσματικό αν επέλεγαν να δημοσιεύσουν φωτογραφίες, οι οποίες είτε δεν έχουν καλό φωτισμό είτε ο χρήστης πραγματοποιεί διάφορους μορφασμούς του προσώπου του. Φυσικά, επιθυμητό θα ήταν, εάν ο χρήστης διατηρεί πολλούς λογαριασμούς σε παραπάνω δηλαδή από ένα κοινωνικό δίκτυο, να διαθέτει διαφορετικές φωτογραφίες προφίλ σε καθένα από αυτά. Επίσης, οι χρήστες, προκειμένου να προστατευτούν όσο το δυνατόν καλύτερα, μπορούν να χρησιμοποιήσουν εργαλεία με τα οποία είτε να κρυπτογραφούν τις εικόνες τους, όπου θα είναι αναγνωρίσιμες από ανθρώπους αλλά όχι από μηχανές, είτε να τις μετατρέπουν σε άλλες μορφές τύπου καρικατούρα. Μία άλλη πρακτική, η οποία από την μεριά της μπορεί να αποτρέψει τον παραπάνω κίνδυνο, αναφέρεται στην πολιτική που επιλέγουν να ακολουθήσουν τα κοινωνικά δίκτυα. Για να γίνουμε πιο συγκεκριμένοι, οι ιστοσελίδες κοινωνικής δικτύωσης καλό θα ήταν να απαγορεύουν την μαζική αποθήκευση λογαριασμών και κατ' επέκταση την αποθήκευση φωτογραφιών. Αποτελεσματικό, επίσης θα ήταν να υιοθετήσουν την τεχνική " CAPTCHA " σύμφωνα με την οποία ζητείται από τον χρήστη να πληκτρολογήσει μία φράση η οποία αποτελείται γράμματα και αριθμούς και δεν είναι ιδιαίτερα ευανάγνωστη. Η παραπάνω διαδικασία πιστοποιεί κατά κάποιο τρόπο την ταυτότητα του χρήστη και ως αποτέλεσμα εμποδίζει την δημιουργία πλαστών λογαριασμών από "ρομπότ" υπολογιστές, οι οποίοι από τη μεριά τους θα αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα αλλά και σε φωτογραφίες χρηστών. Επιπρόσθετα, η παραμετροποίηση των προκαθορισμένων ρυθμίσεων του λογαριασμού του κάθε χρήστη - μέλους, σχετικά με το ποιός έχει πρόσβαση στις προσωπικές τους φωτογραφίες, αλλά και με το ποιός μπορεί να κοινοποιήσει φωτογραφίες δικές τους, αποτελούν πρακτικές αποδοτικές στην αντιμετώπιση της συγκεκριμένης απειλής. Τέλος, σημαντικό είναι οι χρήστες να προσέχουν ιδιαιτέρως τις φωτογραφίες που δημοσιεύουν και κυρίως το περιεχόμενο αυτών, εάν επιθυμούν τη βέλτιστη για αυτούς προστασία της ιδιωτικότητας τους.

3.5 Επισήμανση χρήστη σε φωτογραφίες άλλων χρηστών χωρίς την συγκατάθεσή του (Linkability from image Metadata, Tagging and Cross-profile Images)

3.5.1 Κίνδυνοι που παραμονεύουν

Δεν είναι λίγα τα κοινωνικά δίκτυα, τα οποία επιτρέπουν τόσο τη δημοσίευση των φωτογραφιών χρηστών από τρίτους, όσο και την επισήμανσή τους, χωρίς πολλές φορές την συγκατάθεσή τους. Όταν αναφερόμαστε στην επισήμανση κάποιου χρήστη, κάνουμε λόγο για γνωστοποίηση είτε του ονόματός του, είτε της ηλεκτρονικής του διεύθυνσης, είτε ακόμη και της διεύθυνσης του λογαριασμού του στην συγκεκριμένη ιστοσελίδα κοινωνικής δικτύωσης. Συνηθισμένο είναι το ερώτημα πολλών ανθρώπων, με το ποιόν μπορεί κάποιος χρήστης να επισημάνει στις φωτογραφίες αυτές που δημοσιεύονται στα κοινωνικά δίκτυα. Η απάντηση είναι, πως ο χρήστης από την μεριά του μπορεί να επισημάνει τον οποιοδήποτε, ακόμη και κάποιον ο οποίος δεν διαθέτει καν λογαριασμό σε τέτοιες ιστοσελίδες κοινωνικής δικτύωσης. Βέβαια, εάν συμβεί κάτι τέτοιο, δηλαδή επισημανθεί κάποιος που δεν διαθέτει λογαριασμό, τότε μια ειδοποίηση θα αποσταλεί στην ηλεκτρονική διεύθυνση αυτού του ατόμου, ότι ο συγκεκριμένος χρήστης τον επισήμανε σε κάποια φωτογραφία. Οι κίνδυνοι, όμως δεν σταματάνε εδώ, αφού ακόμη και αν ο χρήστης είναι ιδιαίτερα προσεχτικός και λαμβάνει όλα τα απαραίτητα μέτρα διαφύλαξης της ιδιωτικότητας του, πάλι μπορεί να πέσει εύκολα στην παγίδα αποκάλυψης προσωπικών του στοιχείων και δεδομένων. Αυτό είναι εύκολο να πραγματοποιηθεί, διότι ακόμη και αν ο ίδιος δεν κοινοποιεί προσωπικές του φωτογραφίες, κάποιος φίλος του ή κάποιος τρίτος έχει την δυνατότητα να δημοσιεύσει φωτογραφίες και να τον επισημάνει εν' αγνοία του. Δυστυχώς, τα κοινωνικά δίκτυα, τα οποία διαθέτουν ρυθμίσεις σχετικές με επισημάνσεις χρηστών σε φωτογραφίες αλλά και γεωγραφικές τοποθεσίες είναι πολύ λίγα. Επιπλέον, μία ακόμη απειλή που έχει να κάνει με τη δημοσίευση φωτογραφιών, αφορά τα μεταδεδομένα (metadata) μιας φωτογραφίας. Για να γίνουμε πιο συγκεκριμένοι, πολλά είδη φωτογραφικών μηχανών παράγουν

φωτογραφίες, οι οποίες εκτός από το περιεχόμενό τους, παρουσιάζουν στην φωτογραφία και τον σειριακό αριθμό του προϊόντος. Ας μην ξεχνάμε, τη δημοσιότητα και τις διαστάσεις που είχε πάρει το θέμα, της παράνομης κυκλοφορίας γνωστού μυθιστορήματος από τον μη εξουσιοδοτημένο εκδοτικό οίκο. Ευτυχώς, μέσω των φωτογραφιών που περιείχαν μέσα σε όλα και τον σειριακό αριθμό της φωτογραφικής μηχανής, κατάφεραν να εντοπίσουν τον δράστη.

3.5.2 Τρόποι αντιμετώπισης και προστασίας από την απειλή της επισήμανσης, χωρίς την συγκατάθεση του χρήστη

Πρώτα από όλα, οι ιστοσελίδες κοινωνικής δικτύωσης καλό θα ήταν να προωθούν μηχανισμούς προστασίας της ιδιωτικότητας των χρηστών. Το μεγαλύτερο πρόβλημα των χρηστών έγκειται στο γεγονός, ότι αδυνατούν να ελέγξουν το δικαίωμα της προσωπικής τους προβολής. Πιο αναλυτικά, οι χρήστες πολλές φορές παρουσιάζονται σε φωτογραφίες τρίτων, χωρίς όμως να έχει προηγηθεί κάποιου είδους συγκατάθεση των ίδιων. Το συγκεκριμένο πρόβλημα βέβαια, μπορεί να λυθεί πλέον, εάν ο χρήστης διαλέξει μία από τις επιλογές, που το κοινωνικό δίκτυο του προσφέρει. Οι επιλογές αυτές είναι τρεις, εκ των οποίων στην πρώτη επιλογή, ο χρήστης μπορεί να επισημανθεί από οποιονδήποτε, χωρίς να χρειάζεται η συγκατάθεσή του. Η επιλογή αυτή, αποτελεί και την προκαθορισμένη επιλογή που υφίσταται στις ρυθμίσεις του λογαριασμού ενός χρήστη. Η δεύτερη επιλογή αναφέρεται στην συγκατάθεση του χρήστη, πριν από οποιαδήποτε επισήμανση. Πιο συγκεκριμένα, όταν οποιοσδήποτε χρήστης επιθυμεί να επισημάνει τον συγκεκριμένο χρήστη, ζητείται μέσω της ηλεκτρονικής αλληλογραφίας συνήθως η συγκατάθεσή του, όπου εάν την επιβεβαιώσει, τότε και μόνο πραγματοποιείται η επισήμανσή του στη συγκεκριμένη φωτογραφία. Η τρίτη και τελευταία επιλογή τώρα, αφορά την δυνατότητα που έχει ο χρήστης να απαγορεύει κάθε είδους επισήμανση, είτε αυτή προέρχεται από κάποιον φίλο του μέσα στο κοινωνικό δίκτυο, είτε από κάποιον τρίτο - άγνωστο για τον χρήστη μέλος του δικτύου. Επιπλέον, μία ακόμη ενέργεια, που θα μπορούσε να πραγματοποιήσει ένας χρήστης, για να ενισχύσει την προστασία της

ιδιωτικότητας του, αφόρα την παραμετροποίηση κάποιων ρυθμίσεων στην καρτέλα των ρυθμίσεων της ιδιωτικότητας (privacy settings). Για να γίνουμε πιο συγκεκριμένοι, μέσα στις ρυθμίσεις που αφορούν την ιδιωτικότητα του χρήστη, υπάρχει ένα σημείο που αναφέρεται, πως η εταιρία του συγκεκριμένου κοινωνικού δικτύου (Facebook), όταν εντοπίσει φωτογραφικό υλικό που μοιάζει σε κάποιον συγκεκριμένο χρήστη προτείνει αυτόματα την επισήμανσή του ονόματός του. Έτσι λοιπόν, ο κάθε χρήστης καλό θα ήταν να μελετήσει πολύ προσεχτικά τις ρυθμίσεις του λογαριασμού του και να τις διαμορφώσει όπως ο ίδιος επιθυμεί.

3.6 Δυσκολία για πλήρη διαγραφή προφίλ (Difficulty of Complete Account Deletion)

3.6.1 Ανάλυση και υποψήφιες απειλές

Πολλές φορές, οι χρήστες του διαδικτύου γίνονται μέλη σε διάφορες ιστοσελίδες κοινωνικής δικτύωσης, στη συνέχεια όμως για προσωπικούς τους λόγους επιθυμούν την αποχώρηση και την πλήρη διαγραφή τους από τα συγκεκριμένα δίκτυα. Τι γίνεται όμως, όταν επιθυμούν να απενεργοποιήσουν τον λογαριασμό τους και κατά πόσο είναι εφικτή η οριστική διαγραφή ενός προφίλ ; Οι χρήστες συχνά επιθυμούν να διαγράψουν τους λογαριασμούς τους από τα διάφορα κοινωνικά δίκτυα, κάτι το οποίο ενώ στην αρχή μπορεί να φαίνεται εύκολο, στην πραγματικότητα αποτελεί μια πολύπλοκη διαδικασία. Αρχικά, οι χρήστες έχουν την δυνατότητα να αφαιρέσουν και να διαγράψουν πληροφορίες και δεδομένα του λογαριασμού τους, όπως για παράδειγμα όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, φωτογραφίες κλπ. Αντίθετα, δευτερεύουσες πληροφορίες, όπως δημόσια σχόλια σε προφίλ άλλων χρηστών ή φωτογραφίες που έχει επισημανθεί από τρίτους παραμένουν και δεν διαγράφονται. Από την μεριά τους τα κοινωνικά δίκτυα, στην πολιτική προστασίας τους αναφέρουν πως ακόμη και αν κάποιος χρήστης διαγράψει πληροφορίες από το προφίλ του, αυτές δεν διαγράφονται πλήρως και οι διαχειριστές της εταιρείας

κρατάνε αντίγραφα ασφάλειας για κάποιο χρονικό διάστημα. Δυστυχώς, όμως δεν αναφέρουν πόσο μακρύ είναι αυτό το χρονικό διάστημα. Επίσης, συχνό είναι το φαινόμενο, όπου οι χρήστες δεν διαγράφουν, αλλά απενεργοποιούν τον λογαριασμό τους. Με πιο απλά λόγια, οι χρήστες απενεργοποιούν τον λογαριασμό τους για κάποιο χρονικό διάστημα, όταν όμως αποφασίσουν να το ξαναενεργοποιήσουν εμφανίζονται και πάλι όλες οι φωτογραφίες, οι πληροφορίες, ακόμη και τα σχόλια σε προφίλ άλλων χρηστών. Δυστυχώς, ο χρήστης αδυνατεί να ελέγξει πλήρως την ταυτότητά του μέσα σε ένα κοινωνικό δίκτυο. Αυτό συμβαίνει, διότι αντίγραφα ασφαλείας του λογαριασμού του κρατούνται για πολύ μεγάλο χρονικό διάστημα, έτσι αν ο χρήστης πραγματοποιήσει κάποιο άσχημο σχόλιο, είτε δημοσιοποιήσει μια φωτογραφία που τελικά δεν ήθελε, είναι πολύ δύσκολο να τα διαγράψει πλήρως. Με απλά λόγια, ο χρήστης δεν μπορεί να κάνει χρήση του δικαιώματος που έχει να είναι ο κύριος υπεύθυνος των προσωπικών του δεδομένων, ώστε να τα τροποποιεί και να τα διαγράφει όποτε και όταν αυτός το επιθυμεί. Παρόλα αυτά τα προβλήματα που δημιουργούνται με την χρήση των κοινωνικών δικτύων, αλλά την αδυναμία προστασίας προσωπικών δεδομένων, οι νομοθετικές διατάξεις της εκάστοτε χώρας, αλλά και ολόκληρης της Ευρωπαϊκής Ένωσης τείνουν σε ένα έργο ενίσχυσης της προστασίας της ιδιωτικότητας των χρηστών.

3.6.2 Τεχνικές και προτεινόμενες οδηγίες

Η πρώτη και κυριότερη ενέργεια που θα ήταν καλό να πραγματοποιηθεί, είναι να δημιουργηθούν όλα εκείνα τα απαραίτητα εργαλεία, με τα οποία όλοι οι χρήστες θα έχουν την δυνατότητα να απενεργοποιήσουν και να διαγράψουν πλήρως τους λογαριασμούς τους. Οι δηλώσεις για την πολιτική της ιδιωτικότητας που ακολουθούν όλες αυτές οι ιστοσελίδες κοινωνικής δικτύωσης, θα πρέπει να παρουσιάζονται με ευνόητους και κατανοητούς όρους προς τους χρήστες. Επιπλέον, αποτελεσματικό θα ήταν να τους προτείνουν και συνδέσμους προς άλλους δικτυακούς τόπους, όπου θα υπάρχουν αναλυτικές οδηγίες για το πως κάποιος μπορεί να διαχειριστεί τα προσωπικά του δεδομένα και σχόλια, τόσο στον δικό του λογαριασμό, όσο και στους λογαριασμούς των φίλων του. Ο κάθε χρήστης, θα πρέπει να έχει την δυνατότητα να διαγράψει πλήρως όλα του τα δεδομένα, οποιαδήποτε στιγμή το επιθυμήσει.

Επιπλέον, όπως έχουμε ήδη αναφέρει και παραπάνω, χρήσιμο θα ήταν ο χρήστης να προνοεί και να παραμετροποιεί τις προκαθορισμένες ρυθμίσεις, στοχεύοντας έτσι στον καλύτερο δυνατό έλεγχο του λογαριασμού του. Ακόμη, από την μεριά των κοινωνικών δικτύων, αποδοτικό θα ήταν να υπάρχει πλήρη διαφάνεια με το πως διαχειρίζονται οι υπεύθυνοι αυτών των εταιρειών τα προσωπικά στοιχειά και δεδομένα των χρηστών. Καλό θα ήταν, να παρουσιάζεται σε όλα τα μέλη του δικτύου μια ξεκάθαρη περιγραφή των διαφορών μεταξύ απενεργοποίησης κάποιου λογαριασμού και μεταξύ πλήρους τερματισμού και διαγραφής. Επίσης, μια χρήσιμη πληροφορία για όλους, που ακόμη παραμένει αναπάντητη είναι για πόσο χρονικό διάστημα κρατούνται αντίγραφα ενός προφίλ, από την μέρα της απενεργοποίησης του και μετά. Στις μέρες μας, στα κοινωνικά δίκτυα υπάρχει, τόσο η επιλογή της απενεργοποίησης, όσο και της διαγραφής. Δυστυχώς όμως, ακόμη και εάν επιλέξουμε την διαγραφή, δεν υπάρχει κάποια επίσημη "εγγύηση" ότι αυτό θα συμβεί. Αναλυτικότερα, όταν ένας χρήστης επιθυμήσει να διαγράψει το προφίλ του, τότε πραγματοποιεί κάποιες συγκεκριμένες ενέργειες και για δύο εβδομάδες το απενεργοποιεί. Μέσα όμως στις δύο εβδομάδες αυτές, εάν το επιθυμεί, έχει τη δυνατότητα επανενεργοποίησής του. Εάν πάλι δεν συμβεί κάτι τέτοιο, υποστηρίζεται ότι μετά από αυτές τις δεκαπέντε μέρες , το προφίλ του χρήστη διαγράφεται. Από την άλλη μεριά, υπάρχουν αξιοσημείωτες αμφιβολίες ότι κάτι τέτοιο δεν πραγματοποιείται, αφού κανείς δεν γνωρίζει αν οι διαχειριστές των ιστοσελίδων αυτών όντως τα διαγράφουν. Κλείνοντας, θα πρέπει να υπογραμμιστεί το γεγονός, όπου αν ο χρήστης απενεργοποιήσει το λογαριασμό του και δεν το διαγράψει, οι υπόλοιποι χρήστες διατηρούν το δικαίωμα αφ' ενός να τον προσκαλούν σε διάφορες εκδηλώσεις, αφ' ετέρου να τον επισημάνουν σε σχόλια αλλά και φωτογραφίες.

3.7 Υπόλοιποι κίνδυνοι και απειλές που δεν σχετίζονται με την ιδιωτικότητα

Στη ζωή, όπως και στην τεχνολογία φυσικά, σε κάθε δράση υπάρχει και μία αντίδραση όπως συνηθίζεται να λένε. Η εξέλιξη του διαδικτύου αλλά και των κοινωνικών δικτύων δεν έφεραν απλά τους ανθρώπους κοντά, καθώς διευκόλυναν

την επικοινωνία τους στο έπακρο, δημιούργησαν κιόλας μια πληθώρα κινδύνων και απειλών. Συγκεκριμένα, η διάδοση των κοινωνικών δικτύων συνοδευόταν από μία μεγάλη ποικιλία κινδύνων, που αυτοί από την μεριά τους, είτε αφορούσαν την ιδιωτικότητα των χρηστών, είτε κοινωνικές απειλές κλπ. Παραδοσιακοί κίνδυνοι, που εμφανίζονται τόσο στο διαδίκτυο, όσο και στις ιστοσελίδες κοινωνικής δικτύωσης, μπορούν να επιφέρουν καταστροφικές συνέπειες. Κλασσικά παραδείγματα τέτοιων κινδύνων αποτελούν οι επιθέσεις Spam (SNS Spam), οι συλλογές δεδομένων των χρηστών από διαφορετικά κοινωνικά δίκτυα (SNS Aggregators), καθώς επίσης και η διασπορά ιών. Επιπλέον, καλό θα ήταν να υπογραμμιστούν και οι απειλές, οι οποίες σχετίζονται με τις ψηφιακές ταυτότητες χρηστών. Δυστυχώς, δεν είναι λίγα τα παραδείγματα της δημιουργίας των ψεύτικων προφίλ, της διαρροής των πληροφοριών και δεδομένων, όπως επίσης και του φαινομένου Phishing. Με τον όρο αυτό, αναφερόμαστε στο φαινόμενο κατά το οποίο πραγματοποιούνται "επιθέσεις" στους χρήστες, χωρίς αυτοί να καταλάβουν το παραμικρό, με στόχο την παράνομη απόκτηση του ονόματος ή του κωδικού ενός χρήστη σε μία ιστοσελίδα, καθώς και των αριθμών πιστωτικών του καρτών. Επιπρόσθετα, μεγάλες και σημαντικές διαστάσεις άρχισε να παίρνει και το φαινόμενο των κοινωνικών απειλών μέσα στα κοινωνικά δίκτυα. Για να γίνουμε πιο συγκεκριμένοι, επιθέσεις κοινωνικής μηχανής όπως συνηθίζεται να αποκαλούνται (Corporate Espionage), ή επανειλημμένες και σκόπιμες επιβλαβείς πράξεις με χρήση της τεχνολογίας (Bullying) ή ακόμη και εκφοβιστικές συμπεριφορές (Stalking) αποτελούν μερικά από τα πιο φανερά παραδείγματα. Επιπλέον, θα ήταν καλό να τονιστεί η σημασία του κινδύνου γύρω από την χρήση των κοινωνικών δικτύων από ανήλικα παιδιά. Εάν και υφίσταται όριο ηλικίας για την πρόσβαση σε αυτού του είδους τις ιστοσελίδες, παρόλα αυτά είναι πολύ δύσκολο, για να μην πούμε σχεδόν ακατόρθωτο να ελεγχθεί πραγματικά η ηλικία του χρήστη. Ωστόσο, οι γονείς θα πρέπει να είναι ιδιαίτερα προσεχτικοί, αφού τόσο η επαφή με ακατάλληλο υλικό και ανθρώπους , όσο και ο εθισμός στα κοινωνικά δίκτυα των παιδιών τους, μπορεί να οδηγήσει σε τραγικές συνέπειες, αλλά και καταστάσεις. Όλες οι παραπάνω απειλές, που αναφέρθηκαν, μπορούν να γίνουν πολύ επικίνδυνες, εάν δεν ληφθούν τα κατάλληλα μέτρα. Οδηγίες και μέτρα προστασίας έχουν παρουσιαστεί και παραπάνω και αποτελεσματικό θα ήταν να υιοθετηθούν από όλους τους χρήστες, επιτυγχάνοντας έτσι την βέλτιστη προστασία τους. Επιγραμματικά, να αναφέρουμε πως η σωστή ενημέρωση και εκπαίδευση των χρηστών, η λήψη μέτρων που θα ενδυναμώσουν την προστασία του κάθε χρήστη, η

παραμετροποίηση βασικών ρυθμίσεων, αλλά κυρίως η προσεχτική χρήση των κοινωνικών δικτύων αυτών, αποτελούν μερικά από τα πιο κλασσικά παραδείγματα προληπτικών μέτρων.

3.8 Συγκεντρωτική περιγραφή όλων των κινδύνων

Κατά τη διάρκεια του παρόντος κεφαλαίου, πραγματοποιήθηκε λεπτομερής αναφορά των πιο βασικών κινδύνων που απειλούν την αξία της ιδιωτικότητας των χρηστών. Στη συνέχεια, ακολουθεί ένας συγκεντρωτικός πίνακας, στον οποίο διαφαίνονται τόσο οι κίνδυνοι που αφορούν την ιδιωτικότητα των χρηστών μέσα σε ένα κοινωνικό δίκτυο, όσο και κίνδυνοι που απειλούν άλλα χαρακτηριστικά των χρηστών.

Κίνδυνοι	**Απειλές**	**Προτάσεις-Λύσεις**
Αποθήκευση & μελέτη προφίλ απο τρίτους (όνομα, γεωγραφική τοποθεσία κλπ)	Ιδιωτικότητα των χρηστών	Προσοχή στις πληροφορίες που δημοσιοποιούμε
Δευτερεύουσα αποθήκευση πληροφοριών (IP, τύπος φυλλομετρητή κλπ)	Ιδιωτικότητα των χρηστών	Παραμετροποίηση προκαθορισμένων ρυθμίσεων
Αναγνώριση φυσικών προσώπων (φωτογραφίες προφίλ)	Ιδιωτικότητα των χρηστών	Προσεχτική κοινοποίηση προσωπικών φωτογραφιών
C.B.I.R. (Αποκάλυψη προσωπικών στοιχείων μέσα απο φωτογραφικό υλικό)	Ιδιωτικότητα των χρηστών	Δικαιώματα πρόσβασης σε φωτογραφίες και προσωπικά δεδομένα
Επισήμανση χρήστη με ή χωρις στην συγκατάθεσή του σε φωτογραφίες	Ιδιωτικότητα των χρηστών	Παραμετροποίηση ρυθμίσεων του κοινωνικού δικτύου
Επιθέσεις Spam - Ιοί	Λογισμικό των χρηστών	Λογισμικά Προστασίας
Επιθέσεις Phishing - Διαρροή πληροφοριών	Ψηφιακή ταυτότητα	Συχνή αλλαγή κωδικών
Εκφοβιστικές συμπεριφορές - Βλαβερές πράξεις με χρήση τεχνολογίας	Κοινωνικές απειλές	Σωστή ενημέρωση και εκπαίδευση

Πίνακας (1) - Βασικοί κίνδυνοι & οι λύσεις αυτών στα κοινωνικά δίκτυα

Όπως περιγράφεται ξεκάθαρα και στον πίνακα (1), οι χρήστες των κοινωνικών δικτύων έχουν πολλούς λόγους να ανησυχούν κατά την διάρκεια της πλοήγησής τους μέσα στους ιστοτόπους αυτούς (Facebook, Twitter, Google+, LinkedIn κλπ). Απειλές,

οι οποίες σχετίζονται απόλυτα με την ιδιωτικότητα, όπως η αποθήκευση και μελέτη προφίλ απο τρίτους, αλλά και η δευτερεύουσα αποθήκευση πληροφοριών αποτελούν αντιπροσωπευτικά παραδείγματα. Για την αντιμετώπισή τους, προτείνονται, η προσοχή στις πληροφορίες που δημοσιεύουν οι χρήστες, αλλά και η παραμετροποίηση βασικών ρυθμίσεων. Παρόλ' αυτα, η ιδιωτικότητα των χρηστών συνεχίζει να κινδυνεύει τόσο απο την αναγνώριση φυσικών προσώπων, όσο και απο την απο κάλυψη προσωπικών στοιχείων μέσα από φωτογραφικό υλικό. Ωστόσο, με την προσεχτική κοινοποίηση φωτογραφικού υλικού και την ρύθμιση περιορισμένης πρόσβασης σε αυτό, οι παραπάνω κίνδυνοι μπορούν εύκολα να αντιμετωπιστούν. Ένας τελευταίος κίνδυνος που αφορά την ιδιωτικότητα, όμως εξίσου σημαντικός είναι αυτός της επισημάνσης του χρήστη σε δημοσιεύσεις και φωτογραφίες με ή χωρίς την συγκατάθεσή του. Ενδεικτικός τρόπος αντιμετώπισης της παραπάνω απειλής αποτελεί η παραμετροποίηση ρυθμίσεων που παρέχει το κάθε δίκτυο. Ωστόσο, οι κίνδυνοι δεν σταματούν εδώ, αφού οι επιθέσεις σπαμ και οι ιοί δεν παύουν να παραβιάζουν το λογισμικό των χρηστών, καθώς επίσης και οι επιθέσεις Phishing σε συνδιασμό με την διαρροή πληροφοριών απειλούν την ψηφιακή ταυτότητα του εκάστοτε χρήστη. Λογισμικά προστασίας γνωστών εταιρειών , όπως και η συχνη αλλαγή κωδικών πρόσβασης συντελούν στην προστασία των προηγούμενων κινδύνων. Τέλος, οι εκφοβιστικές συμπεριφορές και οι βλαβερές πράξεις με την χρήση τεχνολογίας αποτελούν κονωνικές απειλές, οι οποίες απο την μεριά τους θέτουν σε κίνδυνο τόσο το χρήστη, όσο και τον εξοπλισμό που χρησιμοποιεί, όμως με την ορθή ενημέρωση και εκπαίδευση ακόμη και αυτά μπορούν να αποφευχθούν.

Κεφάλαιο 4: Συγκριτική αξιολόγηση των μηχανισμών και πολιτικών προστασίας περί ιδιωτικότητας σε δημοφιλή κοινωνικά δίκτυα

4.1 Τα πιο δημοφιλή κοινωνικά δίκτυα

Στις μέρες μας, όπως άλλωστε έχει ήδη αναφερθεί, τόσο η διάδοση, όσο και η χρήση των κοινωνικών δικτύων αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας. Άντρες και γυναίκες ανεξαρτήτου ηλικίας γίνονται μέλη στα διάφορα κοινωνικά δίκτυα και αφιερώνουν μεγάλο μέρος από τον προσωπικό τους χρόνο στην ενασχόλησή τους με αυτά. Τα κοινωνικά δίκτυα, όμως δεν εμφανίστηκαν τώρα πρόσφατα, αλλά η ιστορία τους ξεκινάει από τα μέσα της δεκαετίας του '90 (Παπαβασιλείου, Ραπτοπούλου 2011). Από τα πρώτα κοινωνικά δίκτυα που εμφανίστηκαν ήταν το “The WELL” το 1985, στη συνέχεια ακολούθησαν το 1994 τα “Theglobe.com” και "GeoCities" και το 1995 το “Tripod.com”. Η νέα γενιά κοινωνικών δικτύων εμφανίστηκε το 2001 με το Ryze.com, όπου αποσκοπούσε οι χρήστες του να αξιοποιούν τα επιχειρηματικά τους δίκτυα. Η ιδέα αυτή ποτέ δεν απέκτησε μεγάλη δημοσιότητα, ενώ από το 2003, αναπτύχθηκαν πολλές νέες υπηρεσίες κοινωνικής δικτύωσης και εμφανίστηκε ο όρος YASNS: «Yet Another Social Networking Service». Χαρακτηριστικά μπορούμε να αναφέρουμε τα δίκτυα LinkedIn, Visible Path, and Xing, Dogster**,** Care2**,** Couchsurfing**,** MyChurch**.** Καθώς η τεχνολογία εξελισσόταν και όλο και περισσότεροι άνθρωποι αποκτούσαν πρόσβαση στο διαδίκτυο, κοινωνικά δίκτυα όπως το MySpace και το HiFive, άρχισαν να γίνονται δημοφιλή και αναγνωρίσιμα. Το Facebook ξεκίνησε στις αρχές του 2004 ως ένα κοινωνικό δίκτυο μόνο για τους φοιτητές του Harvard. Από το Σεπτέμβριο του 2005, άρχισε να ανοίγει στο κοινό. Σήμερα, μερικά από τα πιο δημοφιλή κοινωνικά δίκτυα είναι το Facebook, το οποίο έχει κατακτήσει και την πρώτη θέση με 700.000.000 εκτιμώμενους μοναδικούς

χρήστες μηνιαία[3], ακολουθεί το Twitter, ενώ λίγο πιο κάτω στην κατάταξη βρίσκεται Google +. Στη συνέχεια, θα μελετήσουμε και θα παρουσιάσουμε τις τεχνικές προστασίας που αφορούν την ιδιωτικότητα των χρηστών, που έχουν υιοθετήσει αυτές οι ιστοσελίδες κοινωνικής δικτύωσης.

4.2 Facebook

4.2.1 Εισαγωγή

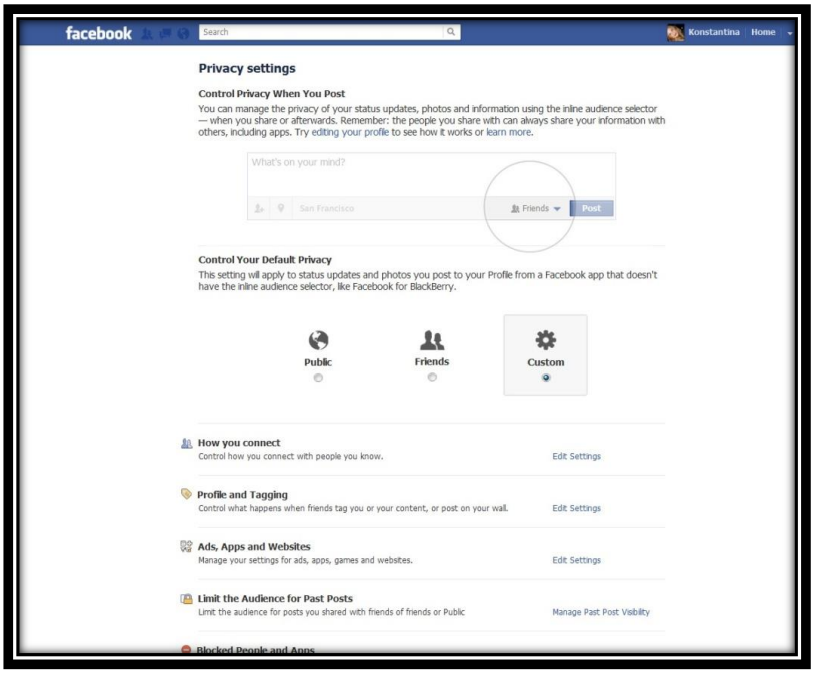
Το Facebook, από τις 4 Φεβρουαρίου του έτους 2004 που πρωτοεμφανίστηκε, αποτελεί μέχρι και σήμερα, οχτώ χρόνια μετά, το πιο διάσημο κοινωνικό δίκτυο παγκοσμίως. Καθημερινά χιλιάδες είναι οι χρήστες, οι οποίοι κάνουν χρήση της συγκεκριμένης ιστοσελίδας κοινωνικής δίκτυωσης. Πιο αναλυτικά, σύμφωνα με ανακοίνωση της εταιρείας Facebook τον Δεκέμβριο του 2011, γνωστοποίησε πως 432 εκατομμύρια ενεργοί χρήστες καταγράφηκαν μηνιαία στην βάση δεδομένων τους. Το νούμερο αυτό είναι απίστευτα μεγάλο και φανερώνει μια πρωτοφανή ανάπτυξη στον κόσμο του διαδικτύου, αφού απο την χρονιά του 2010 μέχρι τα τέλη του 2011, η ανάπτυξη αυτή άγγιξε το 76% (Παπαπαύλου 2012). Παράλληλα όμως, με την απίστευτη ανάπτυξη του Facebook και την διάδοσή του στους χρήστες του διαδικτύου ήρθαν στην επιφάνεια και μία πληθώρα προβλημάτων. Οι διάφορες αντιδράσεις εστιάστηκαν κυρίως στο βαθμό στον οποίο εκτίθενται οι ίδιοι οι χρήστες και τα προσωπικά τους δεδομένα. Έτσι, σχεδόν όλες οι ιστοσελίδες κοινωνικής δικτύωσης και ιδιαίτερα αυτές, οι οποίες διαθέτουν μεγάλο αριθμό ενεργών χρηστών έχουν υιοθετήσει ένα σύνολο απο πρακτικές και τεχνικές προστασίας τόσο της ιδιωτικότητας των χρηστών, όσο και των προσωπικών τους δεδομένων.

[3] **http://magoulaonline.gr/2011/09/19688**

Εικόνα (1) - Λογότυπο κοινωνικού δικτύου Facebook

4.2.2 Προστασία της ιδιωτικότητας απο την πλευρά των χρηστών

Πρώτα από όλα, καλό θα ήταν να διαχωρίσουμε τις δύο μορφές προστασίας που υφίστανται αυτή την στιγμή στο Facebook. Για να γίνουμε πιο συγκεκριμένοι, ο χρήστης από την μεριά του έχει την δυνατότητα να παραμετροποιήσει ως ένα βαθμό τον τρόπο έκθεσης των προσωπικών του δεδομένων. Από την άλλη μεριά, η εταιρεία Facebook διαθέτει την δική της πολιτική προστασία και οι όροι της βρίσκονται ιεραρχικά υψηλότερα απο αυτούς του χρήστη. Στη συνέχεια, θα αναλυθούν, θα παρουσιαστούν αλλά και θα συγκριθούν και οι δύο τρόποι προστασίας. Ξεκινώντας λοιπόν, αποδοτικό θα ήταν να έχουμε μία εικόνα της εφαρμογής που προσφέρει η εταιρεία Facebook προς τους χρήστες της, όπου με την σειρά τους οι τελευταίοι μπορούν να παραμετροποιήσουν.



Εικόνα (2) - Ρυθμίσεις πρόσβασης στο προφίλ και στις κοινοποιήσεις

Όπως φαίνεται και στην εικόνα (2), ο χρήστης του συγκεκριμένου κοινωνικού δικτύου έχει την δυνατότητα να ρυθμίσει το κοινό που θα αποκτά πρόσβαση στο προφίλ του, όταν ο ίδιος πραγματοποιήσει μία συγκεκριμένη ενέργεια. Αναλυτικότερα, όταν ο χρήστης επιθυμεί να κοινοποιήσει κάποιες προσωπικές του απόψεις ή νέα (status updates), ή να δημοσιοποιήσει φωτογραφίες μπορεί να επιλέξει ποιοί θα έχουν πρόσβαση σε αυτά. Πρόσβαση λοιπόν, είναι δυνατόν να έχει οποιοσδήποτε είναι μέλος της συγκεκριμένης ιστοσελίδας κοινωνικής δικτύωσης, τόσο δηλαδή άτομα που γνωρίζει ο χρήστης όσο και άγνωστα εντελώς προς αυτόν και τους φίλους του. Επίσης, μία δεύτερη επιλογή είναι δικαίωμα πρόσβασης να έχουν μόνο οι φίλοι του χρήστη και η τελευταία επιλογή είναι το δικαίωμα του χρήστη να προσαρμόσει, όπως εκείνος επιθυμεί ποιά άτομα ακόμη και απο τους φίλους του θα είναι εξουσιοδοτημένοι και θα έχουν πρόσβαση στο προσωπικό του προφίλ, αλλά και σε συγκεκριμένες ενέργειες . Στην τρίτη και τελευταία επιλογή ο χρήστης έχει τις εξής επιλογές, είτε το προφίλ του να είναι προσβάσιμο μόνο από φίλους του, είτε μόνο απο φίλους των φίλων του, είτε μόνο απο συγκεκριμένα άτομα απο τους φίλους του, είτε τέλος να έχει πρόσβαση μόνο ο ίδιος [εικόνα 3].

Εικόνα (3) - Ρυθμίσεις προσαρμοσμένου απορρήτου

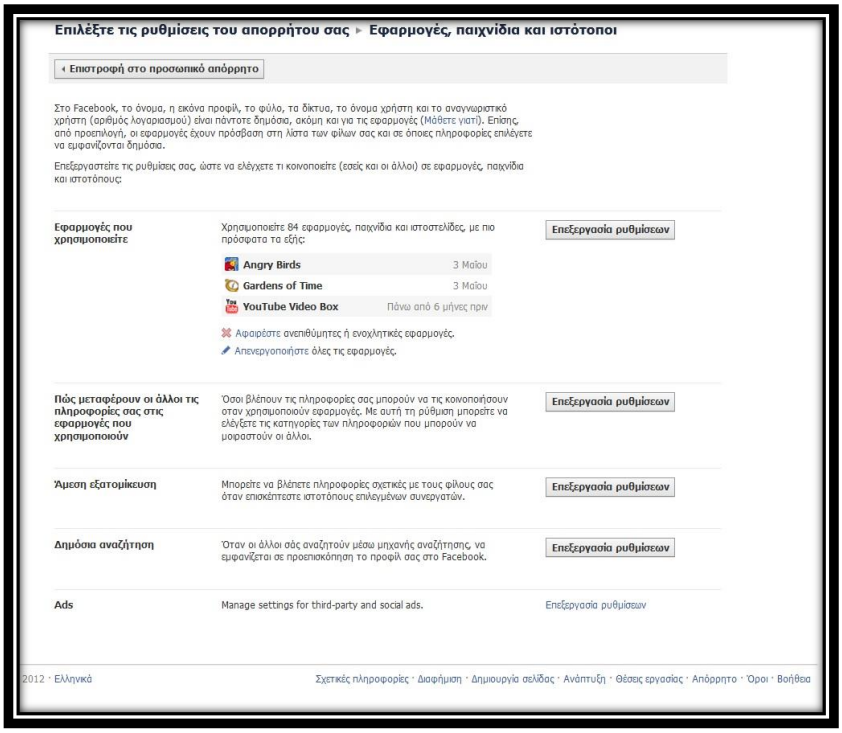
Έπειτα, ο χρήστης μπορεί να επιλέξει τους τρόπους σύνδεσης με όσους γνωρίζει. Για να γίνουμε πιο συγκεκριμένοι, έχει την δυνατότητα να καθορίσει ποιοί μπορούν να τον αναζητήσουν μέσα στο κοινωνικό δίκτυο, ποιοί μπορούν να του στέλνουν προσωπικά μηνύματα και τέλος ποιοι μπορούν να αναζητήσουν το προσωπικό του προφίλ μέσα στο διαδίκτυο, χρησιμοποιώντας την ηλεκτρονική του διεύθυνση [εικόνα 4].

Εικόνα (4) - Δυνατότητες επικοινωνίας και σύνδεσης στο Facebook

Επιπλέον, υπάρχει η επιλογή οι χρήστες - μέλη του κοινωνικού δικτύου Facebook να ρυθμίσουν τι θα συμβαίνει, όταν οι φίλοι τους προσθέτουν ετικέτα στο χρήστη ή στο περιεχόμενό του ή επιθυμούν να δημοσιεύσουν κάτι στον τοίχο του. Όπως φαίνεται και στην εικόνα (5) παρακάτω, μπορεί να καθορίσει ποιός μπορεί να κοινοποιήσει δεδομένα/πληροφορίες στο προφίλ του, ποιός μπορεί να τον επισημάνει σε φωτογραφίες ή μέρη κλπ.

Εικόνα (5) - Ρυθμίσεις επισημάνσεων και ετικετών στο Facebook

Εκτός από όλα τα παραπάνω, ένα μέλος του Facebook δύναται να παραμετροποιήσει τόσο τις ρυθμίσεις των διαφόρων εφαρμογών, παιχνιδιών, διαφημίσεων αλλά και ιστοσελίδων που υπάρχουν μέσα στο κοινωνικό δίκτυο [εικόνα 6], όσο και να περιορίσει το κοινό που είχε και έχει πρόσβαση σε παλαιότερες δημοσιεύσεις του.



Εικόνα (6) - Ρυθμίσεις εφαρμογών και παιχνιδιών τρίτων κατασκευαστών στο Facebook

Τελευταίο, αλλά εξίσου σημαντικό είναι η δυνατότητα του χρήστη να διαχειρίζεται ο ίδιος τα άτομα και τις εφαρμογές που έχει μπλοκάρει [εικόνα 7].

Εικόνα (7) - Ρυθμίσεις μπλοκαρίσματος στο Facebook

4.2.3 Προστασία της ιδιωτικότητας απο την πλευρά της εταιρείας Facebook

Παραπάνω, αναφέρθηκαν όλοι οι τρόποι σύμφωνα με τους οποίους οι χρήστες από την μεριά τους μπορούν να επηρεάσουν και να τροποποιήσουν το κοινό που θα του επιτρέπεται η πρόσβαση στα προσωπικά τους προφίλ. Από την πλευρά της τώρα, η εταιρεία Facebook ακολουθεί δύο βασικές αρχές για την προστασία της ιδιωτικότητας. Η πρώτη αναφέρεται στο γεγονός ότι, ο κάθε χρήστης θα πρέπει να έχει τον έλεγχο για τα προσωπικά του δεδομένα. Ο χρήστης δύναται να επιλέξει ποιες πληροφορίες θα τοποθετήσει στο προφίλ του, συμπεριλαμβανομένων των επαφών και προσωπικών πληροφοριών, φωτογραφιών, συμφερόντων, ομάδων κλπ . Ο ίδιος έχει τον έλεγχο των χρηστών με τους οποίους θέλει να μοιράζεται τις πληροφορίες αυτές μέσω των ρυθμίσεων του απορρήτου (Privacy Settings). Η δεύτερη αρχή αναφέρεται στο γεγονός όπου ο χρήστης θα πρέπει να έχει πρόσβαση σε πληροφορίες που χρησιμοποιούν οι άλλοι αλλά αφορούν τον ίδιο. Επίσης, το Facebook προσφέρει στα μέλη του, όλα εκείνα τα απαραίτητα εργαλεία προστασίας της ιδιωτικής τους ζωής για τον έλεγχο και τον τρόπο με τον οποίο θα μοιράζονται τις πληροφορίες αυτές. Αναλυτικότερα, ας παρουσιάσουμε την πολιτική προστασίας της ιδιωτικότητας που ακολουθεί η εταιρεία Facebook απο την στιγμή που κάποιος χρήστης εγγράφεται στο συγκεκριμένο κοινωνικό δίκτυο. Από την στιγμή, που ο χρήστης πραγματοποιήσει την εγγραφή του στην ιστοσελίδα κοινωνικής δικτύωσης, για να προχωρήσει σε οποιαδήποτε ενέργεια, υποχρεώνεται να συμφωνήσει σε όλους τους όρους που αναγράφονται στην πολιτική απορρήτου. Κατά την διάρκεια της εγγραφής κάποιου χρήστη στο Facebook, του ζητούνται να δώσει ορισμένα προσωπικά του στοιχεία. Αυτά συνήθως είναι το όνομα, το επίθετο, η ηλεκτρονική τους διεύθυνση, ο αριθμός του τηλεφώνου τους, τη φυσική διεύθυνσή, το φύλο, η εκπαίδευση και οποιαδήποτε άλλη προτίμηση. Με την σειρά του το Facebook αποθηκεύει τον τύπο του φυλλομετρητή (browser) των χρηστών και την διεύθυνση του πρωτοκόλλου του διαδικτύου (ip address) τους και τα συλλέγει όλα αυτά σε μια βάση δεδομένων. Επιπλέον, αποθηκεύει ορισμένες πληροφορίες γνωστές και ως "cookies"[4] .

[4] Είδος αρχείων τα οποία δημιουργούνται και αποθηκεύονται στον σκληρό δίσκο του Η/Υ από τα web sites που επισκεπτόμαστε στο internet, με απώτερο σκοπό την αναγνώρισή μας από αυτά την επόμενη φορά που θα επισκεφτούμε την σελίδα.

Ο χρήστης τώρα, που είναι μέλος στο Facebook, έχει την δυνατότητα να δημιουργήσει το προσωπικό του προφίλ, να συνάψει σχέσεις και φιλίες, να στέλνει και να δέχεται προσωπικά μηνύματα, να δημοσιοποιεί φωτογραφίες και βίντεο, να δημιουργεί ομάδες, να δέχεται και να στέλνει προσκλήσεις για διάφορες οργανώσεις και γεγονότα, να παίζει παιχνίδια κλπ. Όλες αυτές τις πληροφορίες, η εταιρεία Facebook έχει το δικαίωμα να τις συλλέξει και να τις χρησιμοποιήσει με σκοπό να προσφέρει στους χρήστες του εξατομικευμένες λειτουργίες, στοχευόμενες διαφημίσεις και υπηρεσίες που ο ίδιος μπορεί να επιθυμεί. Ιδιαίτερη σημασία και προσοχή θα πρέπει να δοθεί στο γεγονός, ότι οποιαδήποτε πληροφορία εισάγει ο κάθε χρήστης στο Facebook γίνεται αποκλειστικά και μόνο με δική του ευθύνη. Συνήθως, οι χρήστες το ξεχνάνε αυτό και συχνά μετατρέπονται σε θύματα απάτης. Αυτό συμβαίνει για τον λόγο ότι, το Facebook δεν μπορεί να ελέγξει τις ενέργειες των άλλων χρηστών με τους οποίους ο χρήστης επιλέγει να μοιράζετε τις σελίδες και τις πληροφορίες του. Ως εκ τούτου, δεν μπορεί και να εγγυηθεί ότι, τα περιεχόμενα της ιστοσελίδας του κάθε χρήστη δεν θα είναι ορατά από αναρμόδια και μη εξουσιοδοτημένα πρόσωπα. Πιο συγκεκριμένα, στην πολιτική του αναφέρει πως δεν φέρει καμία απολύτως ευθύνη για τις αλλαγές που μπορούν να συμβούν στις ρυθμίσεις ιδιωτικότητας (Privacy Settings), για τα μέτρα ασφαλείας της ιστοσελίδας, όπως επίσης και για το γεγονός ότι ακόμη και αν κάποιος χρήστης απενεργοποιήσει το προφίλ του, αυτό μπορεί να παραμένει ακόμη ορατό. Επιπλέον, η εταιρεία Facebook αναφέρει στην πολιτική της ότι δεν μοιράζει τις πληροφορίες των χρηστών - μελών της σε τρίτα μέρη διαφημιστών χωρίς πρώτα την άδειά τους. Παρόλ' αυτά, αναφέρει, πως έχει την δυνατότητα να κοινοποιεί πληροφορίες των χρηστών σε τρίτους περιστασιακά και αυτό όταν η εταιρεία κρίνει πως είναι λογικά απαραίτητο ή νόμιμα απαιτούμενο, για να προσφέρει κάποια υπηρεσία. Για παράδειγμα, η εταιρεία Facebook περιορίζει την πρόσβαση σε πληροφορίες της ιστοσελίδας από μηχανές αναζήτησης και επιτρέπει να φαίνονται μόνο το ονοματεπώνυμο και η φωτογραφία του χρήστη. Ένα ακόμη σημείο, στο οποίο θα πρέπει να δοθεί ιδιαίτερη προσοχή είναι ότι συχνά οι χρήστες του Facebook χρησιμοποιούν εφαρμογές τρίτου τύπου, αγνοώντας τις επιπτώσεις που μπορεί να έχουν. Αναλυτικότερα, οι Πλατφορμικές εφαρμογές αυτές έχουν το δικαίωμα και αποκτούν πρόσβαση στις πληροφορίες του χρήστη. Επιπλέον, οι προγραμματιστές, οι οποίοι έχουν δημιουργήσει και ελέγχουν τις πλατφορμικές εφαρμογές , ίσως να έχουν και αυτοί πρόσβαση στις προσωπικές τους πληροφορίες . Βέβαια, πριν επιτραπεί σε κάποιον πλατφορμικό

προγραμματιστή, να θέσει οποιαδήποτε πλατφορμική εφαρμογή διαθέσιμη στον χρήστη, το Facebook απαιτεί από αυτόν, να έρθει σε συμφωνία, η οποία, δεσμεύει τους προγραμματιστές να σέβονται τις ρυθμίσεις απορρήτου των χρηστών. Παρόλα αυτά, ενώ το Facebook έχει θέσει σε ισχύ τη δέσμευση με συμβόλαιο, και έχει κάνει και άλλα τεχνικά βήματα ,για να περιορίσει την πιθανότητα λάθους χρήσης τέτοιων πληροφοριών, από τους συγκεκριμένους προγραμματιστές, δεν μπορεί να εγγυηθεί ότι κάποιος απο όλους αυτούς, δεν θα αψηφήσει την συμφωνία τους. Σχετικά τώρα με τις διαφημίσεις, η εταιρεία Facebook διαβεβαιώνει ότι δεν παραχωρεί σε εφαρμογές τρίτων ή σε διαφημιστικά δίκτυα το δικαίωμα να χρησιμοποιούν το όνομα ή τη φωτογραφία σας στις διαφημίσεις τους. Αν επιτρέψει κάτι τέτοιο στο μέλλον, η ρύθμιση που επιλέγετε θα καθορίσει πώς θα χρησιμοποιηθούν τα στοιχεία σας[5]. Επίσης, όσο αναφορά τις κοινωνικές διαφημίσεις ισχύουν τα εξής : οι διαφημίσεις αυτές δείχνουν το μήνυμα ενός διαφημιστή δίπλα στις δραστηριότητές σας (π.χ. όταν δηλώνετε ότι σας αρέσει μια σελίδα), οι ρυθμίσεις του προσωπικού σας απορρήτου ισχύουν για τις κοινωνικές διαφημίσεις, αν χρησιμοποιηθεί κάποια φωτογραφία, αυτή θα είναι η φωτογραφία του προφίλ, και όχι κάποια φωτογραφία από τα άλμπουμ και τέλος δεν πουλιούνται οι πληροφορίες των χρηστών σε διαφημιστές. Σ' αυτό το σημείο, καλό θα ήταν να παρουσιάσουμε τους τρόπους με τους οποίους, η εταιρεία του συγκεκριμένου κοινωνικού δικτύου χρησιμοποιεί τις πληροφορίες και τα δεδομένα των χρηστών. Μερικοί απο τους πιθανούς λόγους χρήσης των δεδομένων των χρηστών είναι :

- στο πλαίσιο των προσπαθειών της εταιρείας να παραμείνει ασφαλές το Facebook
- για να ενημερώνεστε σχετικά με δυνατότητες και υπηρεσίες τοποθεσίας (π.χ. ο χρήστης και οι φίλοι του θα ενημερώνονται όταν συμβαίνει κάτι στην περιοχή τους)
- για να μετρήσουνε ή να κατανοήσουνε την αποτελεσματικότητα των διαφημίσεων που εμφανίζονται σε όλους τους χρήστες
- για να πραγματοποιηθούν προτάσεις στους χρήστες της ιστοσελίδας

Τελευταίο, όμως εξίσου σημαντικό είναι το γεγονός όπου, οι χρήστες του κοινωνικού δικτύου Facebook θα πρέπει να γνωρίζουν ποιές από τις προσωπικές του πληροφορίες λαμβάνονται απο την συγκεκριμένη εταιρεία. Οι παρακάτω πληροφορίες εμφανίζονται πάντοτε δημόσια και θεωρούνται δεδομένα που ο κάθε χρήστης έχει

[5] http://www.facebook.com/settings?tab=ads&edited=platform

αποφασίσει να δημοσιοποιήσει. Το όνομα, οι εικόνες προφίλ, το δίκτυο, το αναγνωριστικό και το όνομα χρήστη. Παρόλο που η εταιρεία Facebook μπορεί να χρησιμοποιήσει τις πληροφορίες των χρηστών της, αυτές θα ανήκουν σ'αυτούς για πάντα. Θεωρούνε πολύ σημαντική την εμπιστοσύνη των μελών τους. Γι' αυτό δεν κοινοποιούμε τις πληροφορίες τους σε άλλους, εκτός από τις εξής περιπτώσεις : οι χρήστες έχουν δώσει την άδειά τους, έχουν ειδοποιηθεί σχετικά , ή έχει αφαιρεθεί το όνομα του χρήστη ή άλλα προσωπικά στοιχεία ταυτότητάς του από τις συγκεκριμένες πληροφορίες.

4.3 Twitter

4.3.1 Γενικά

Το Twitter αποτελεί μία ακόμη ιστοσελίδα κοινωνικής δικτύωσης που παράλληλα προσφέρει micro-blogging[6] υπηρεσίες επιτρέποντας στους χρήστες του να ανταλλάσουν μηνύματα, τα οποία στη γλώσσα του Twitter είναι γνωστά ως "Tweets". Τα Tweets δεν είναι τίποτα άλλο από μηνύματα κειμένου με μέγιστο μέγεθος τους 140 χαρακτήρες. Οι χρήστες μπορούν να επιλέξουν, αν τα tweets τους θα είναι ορατά μόνο στην λίστα των φίλων τους, ή θα είναι προσβάσιμα από όλους, το οποίο αποτελεί την προκαθορισμένη επιλογή του Twitter. Για την ανταλλαγή των tweets, ο χρήστης μπορεί να χρησιμοποιήσει, τόσο αυτή καθ'αυτή τη συγκεκριμένη ιστοσελίδα, όσο και την υπηρεσία SMS, αλλά και άλλες εφαρμογές. Η χρήση του Twitter είναι δωρεάν, αν και όπως είναι φυσικό αν κάποιος χρησιμοποιεί υπηρεσίες SMS για αποστολή των tweets του, θα χρεώνει τον τηλεφωνικό του λογαριασμό. Επειδή η χρήση του με αυτόν τον τρόπο όμως είναι ιδιαίτερα διαδεδομένη, το Twitter τιτλοφορείται από πολλούς "το SMS του Internet". Η δημιουργία του αρκετά πρωτότυπου αυτού κοινωνικού δικτύου έλαβε χώρα το 2006 από τον μόλις

[6] http://www.webdesignblog.gr/micro-blogging-what-is-it/
Το *Micro Blogging* είναι μια μορφή blogging αλλά σε πολύ μικρότερη κλίμακα. Ο κάθε micro blogger έχει τη δυνατότητα να κάνει post μικρά μηνύματα *140-200 χαρακτήρων* ανάλογα με την πλατφόρμα. Αυτό που κάνει το micro blogging διαφορετικό, είναι ότι προσφέρει στους χρήστες τη δυνατότητα να κάνουν post χρησιμοποιώντας διάφορα μέσα, όπως *υπολογιστές, κινητά τηλέφωνα* με υποστήριξη *SMS* ή *Wi-Fi*, *messengers* και *email*. Αυτή η πληθώρα επιλογών, σε συνδυασμό με το μικρό μέγεθος των μηνυμάτων, έχει καταστήσει τις micro blogging πλατφόρμες πολύ δελεαστικές, ιδιαίτερα σε χρήστες που θέλουν να εκφραστούν ανά πάσα στιγμή για οτιδήποτε μπορεί να θεωρούν αξιόλογο προς αναφορά.

τριαντάχρονο τότε Jack Dorsey. Έκτοτε, η ιστοσελίδα κερδίζει όλο και περισσότερη δημοτικότητα και σήμερα αποτελεί το δεύτερο κατά σειρά πιο δημοφιλές κοινωνικό δίκτυο.

4.3.2 Η Πολιτική Προστασίας του Twitter

Το twitter, όπως και τα υπόλοιπα κοινωνικά δίκτυα συλλέγουν τα προσωπικά στοιχεία των χρηστών-μελών τους. Το θέμα όμως που απασχολεί όλους είναι το πως αυτές οι πληροφορίες αξιοποιούνται ή χρησιμοποιούνται. Πρώτα απ' όλα, να αναφέρουμε τους τρόπους με τους οποίους, το Twitter συλλέγει τα προσωπικά δεδομένα των χρηστών του. Αυτό συνήθως πραγματοποιείται, είτε απο τις διάφορες ιστοσελίδες που επισκέπτεται ο χρήστης, είτε απο τα SMS, είτε απο τις διάφορες εφαρμογές τρίτου τύπου και όχι. Σ'αυτό το σημείο να αναφέρουμε, πως το Twitter δεν περιέχει διαφημίσεις στη σελίδα του, υπάρχει το ενδεχόμενο όμως, οι διαφημιστές να στραφούν σε κάποιον συγκεκριμένο χρήστη για να προωθήσουν το προϊόν τους, εκμεταλλευόμενοι πληροφορίες που έχουν συλλέξει για αυτόν με βάση τα μηνύματά (Tweets) του. Όταν κάποιο μέλος κάνει χρήση μία απο τις διάφορες υπηρεσίες του κοινωνικού αυτού δικτύου, τότε και σύμφωνα με την πολιτική προστασίας συμβάλλει στην συλλογή, τον χειρισμό, την αποκάλυψη, την μεταφορά και την αποθήκευση των διαφόρων πληροφοριών. Επίσης, στην πολιτική αυτή αναφέρεται το γεγονός ότι εάν κάποιος χρήστης βρίσκεται εκτός των Η.Π.Α. η εταιρεία Twitter μπορεί να χρησιμοποιήσει τα δεδομένα του, τόσο στις Η.Π.Α. , όσο και στις υπόλοιπες χώρες στις οποίες εκτίνεται. Όταν κάποιος χρήστης γίνει μέλος στη συγκεκριμένη ιστοσελίδα κοινωνικής δικτύωσης, τότε κοινοποιεί στην εταιρεία το όνομά του, το ψευδώνυμο του και την ηλεκτρονική του διεύθυνση υποχρεωτικά, τον αριθμό του κινητού τηλεφώνου, την τοποθεσία και μερικά στοιχεία του εαυτού του προαιρετικά. Η εταιρεία αναφέρει, πως το όνομα και το ψευδώνυμο του χρήστη, καθώς και το προφίλ του είναι δημόσια στοιχεία και μπορούν ακόμη να εμφανίζονται στα αποτελέσματα των μηχανών αναζήτησης. Ακόμη, εάν κάποιος χρήστης στείλει κάποιο μήνυμα στην εταιρεία, τότε αυτή κρατάει και καταχωρεί την ηλεκτρονική του διεύθυνση. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στο γεγονός ότι, το Twitter αποτελεί ένα κοινωνικό δίκτυο, το οποίο κατασκευάστηκε ώστε οι χρήστες να

μοιράζονται πληροφορίες και δεδομένα δημόσια, με όλο τον κόσμο. Απο την άλλη μεριά, η εταιρεία, μέσω των ρυθμίσεων που παρέχει, δίνει την δυνατότητα στους χρήστες να τις παραμετροποιήσουν, προστατεύοντας έτσι τα προσωπικά τους μηνύματα (tweets) απο το ευρύ κοινό, κάνοντάς τα γνωστά μόνο στις λίστες των ατόμων που ο ίδιος ο χρήστης έχει επιλέξει. Παρόλ'αυτά, οι διάφοροι χρήστες του Twitter, θα πρέπει να είναι αρκετά προσεχτικοί τόσο με τις πληροφορίες όσο και με τα μηνύματα που κοινοποιούν, καθώς οι παγίδες που πιθανόν να υπάρχουν είναι πολλές. Επιπλέον, η εταιρεία Twitter συλλέγει και επεξεργάζεται ακόμη ένα σύνολο δεδομένων, όπως αυτά της διαδικτυακής διεύθυνσης του χρήστη, τον τύπο του φυλλομετρητή, τις ιστοσελίδες τις οποίες επισκέπτεται, τον τύπο και την εταιρεία του κινητού του τηλεφώνου, καθώς επίσης και των εφαρμογών που συνήθως χρησιμοποιεί. Σε γενικές γραμμές όμως, στην πολιτική προστασίας της εταιρείας Twitter αναφέρεται πως τα προσωπικά δεδομένα και πληροφορίες κάποιου δεν "μοιράζονται" σε τρίτους, παραμόνο αν υπάρξει η συγκατάθεση του ίδιου του χρήστη. Αυτό βέβαια, δεν ισχύει στην περίπτωση όπου ο χρήστης - μέλος έχει επιλέξει τα μηνύματά του (tweets) και οι πληροφορίες του να είναι προσβάσιμες στο ευρύ κοινό (public). Ακόμη, τα προσωπικά προφίλ των χρηστών δεν πουλιούνται σε καμία περίπτωση, εκτός βέβαια και αν η συγκεκριμένη εταιρεία κλείσει και αγοραστεί απο άλλον. Διαγραφή του προφίλ κάποιου χρήστη μπορεί να πραγματοποιηθεί, αρκεί να παραμείνει απενεργοποιημένο τουλάχιστον για 30 ημέρες. Η διαγραφή ενός προφίλ χρειάζεται απο την μεριά της εταιρείας περίπου μία εβδομάδα. Τέλος, η εταιρεία απαγορεύει την χρήση του κοινωνικού δικτύου σε παιδιά κάτω των 13 ετών και αν εντοπιστεί κάποιο τέτοιο γεγονός τότε το προφίλ διαγράφεται άμεσα. Σε περίπτωση επίσης, που η εταιρεία πραγματοποιήσει αλλαγές στην πολιτική προστασίας της ιδιωτικότητας των χρηστών, ενημερώνει τους χρήστες της, είτε μέσω ηλεκτρονικού μηνύματος (email), είτε μέσω κοινοποίησης στο κοινωνικό δίκτυο.

Εικόνα (8) - Λογότυπο κοινωνικού δικτύου Twitter

4.4 Google plus (Google +)

4.4.1 Εισαγωγή

Το Google plus (Google+) είναι πολύ απλά ένα νέο κοινωνικό δίκτυο από την μεγαλύτερη εταιρεία διαδικτυακών υπηρεσιών το οποίο φέρει και το όνομα της. Η Google μετά από κάποιες αποτυχημένες προσπάθειες κοινωνικών δικτύων (π.χ. Buzz, Wave κτλ.) δημιούργησε το Google plus με στόχο να εδραιωθεί και να ανταγωνιστεί άλλα μεγάλα κοινωνικά δίκτυα όπως το Facebook, Twitter κτλ.[7] Το Google + είναι ένα κοινωνικό δίκτυο που προσφέρει η εταιρεία Google σε όλους όσους έχουν ένα λογαριασμό ηλεκτρονικού ταχυδρομείου (gmail), να δημιουργήσουν κύκλους επαφών και να μοιράζονται πράγματα μαζί τους. Είναι μία πλατφόρμα αλληλεπίδρασης μεταξύ χρηστών, που βασικό της χαρακτηριστικό είναι ότι κανείς, έχει την δυνατότητα να μοιράζεται σκέψεις, φωτογραφίες, ιδέες, προτάσεις με τους ανθρώπους που θέλει. Η καινοτομία που έφερε το συγκεκριμένο κοινωνικό δίκτυο ονομάζεται Google+ Hangouts**,** δυνατότητα για ταυτόχρονη συνομιλία (video chat) με τις επαφές σας. Το πρωτοφανές χαρακτηριστικό είναι ότι, η οθόνη αλλάζει ανάλογα με το ποιος μιλάει, κάτι πολύ καλύτερο από το να έχετε πολλαπλές οθόνες με κάμερα ανοιχτές. Εντύπωση προκάλεσε το γεγονός όπου, τον Ιανουάριο του 2012, ο πρόεδρος των Η.Π.Α. Barrack Obama, χρησιμοποίησε την συγκεκριμένη εφαρμογή, ώστε να απαντήσει ευθέως στους πολίτες της Αμερικής. Παρόλο, που η ιστοσελίδα κοινωνικής δικτύωσης Google+ είναι σχετικά καινούργια, αφού μόλις τον Ιούνιο του 2011 έκανε το ντεμπούτό της, η πολιτική προστασίας που ακολουθεί περί ιδιωτικότητας έχει ιδιαίτερο ενδιαφέρον.

[7] http://www.eartboard.com/blog/google-plus/

Εικόνα (9) - Λογότυπου κοινωνικού δικτύου Google+

4.4.2 Πολιτική Απορρήτου

Σύμφωνα με την πολιτική απορρήτου της εταιρείας Google +, οι υπεύθυνοι του συγκεκριμένου κοινωνικού δικτύου συλλέγουν στοιχεία με δύο βασικούς τρόπους. Ο ένας τρόπος, που μοιάζει με αυτούς των άλλων γνωστών κοινωνικών δικτύων, είναι τα στοιχεία που δίνουν οι ίδιοι οι χρήστες - μέλη της ιστοσελίδας κοινωνικής δικτύωσης. Για παράδειγμα, πολλές από τις υπηρεσίες της Google απαιτούν να δημιουργήσουν οι χρήστες έναν λογαριασμό. Με τον λογαριασμό αυτό, ζητούνται συνήθως κάποια προσωπικά στοιχεία, όπως το όνομά, η διεύθυνσή ηλεκτρονικού ταχυδρομείου, ο αριθμός τηλεφώνου ή τα στοιχεία των πιστωτικών καρτών των χρηστών. Σε περίπτωση τώρα, που ο χρήστης επιθυμεί να εκμεταλλευτεί πλήρως την κοινή χρήση λειτουργιών, που παρέχει η συγκεκριμένη εταιρεία, ενδέχεται να του ζητηθεί, να δημιουργήσει ένα δημόσια ορατό προφίλ, το οποίο ενδέχεται να περιλαμβάνει το όνομα και τη φωτογραφία του. Από την άλλη μεριά, η εταιρεία Google+ συλλέγει στοιχεία απο τους ίδιους τους χρήστες, κατά την διάρκεια της πλοήγησής τους στο κοινωνικό δίκτυο. Με αυτόν τον τρόπο, η εταιρεία ενδέχεται να συλλέξει στοιχεία για την συσκευή, μέσω της οποίας ο χρήστης συνδέεται στο κοινωνικό δίκτυο. Στοιχεία όπως το μοντέλο, η έκδοση του λειτουργικού συστήματος, τα μοναδικά αναγνωριστικά της συσκευής και πληροφορίες για το δίκτυο κινητής τηλεφωνίας. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στη συλλογή στοιχείων και ειδικότερα στα αρχεία καταγραφής του διακομιστή του χρήστη. Τα αρχεία αυτά συνήθως περιλαμβάνουν στοιχεία συμβάντων της συσκευής, όπως τυχόν διακοπές λειτουργίας, τη δραστηριότητα του συστήματος, τις ρυθμίσεις της συσκευής, τον τύπο του προγράμματος περιήγησης, τη γλώσσα του προγράμματος περιήγησης, την ημερομηνία ακόμη και την ώρα του αιτήματός σας και τη διεύθυνση αναφοράς. Επίσης, περιλαμβάνουν την διεύθυνση του πρωτοκόλλου του διαδικτύου

(ip address) τους, πληροφορίες γνωστές και ως "cookies" ακόμη και λεπτομέρειες σχετικά με τον τρόπο με τον οποίο οι χρήστες αλληλεπιδρούν με την υπηρεσία, όπως διάφορα ερωτήματά αναζήτησης. Τρόμο ίσως προκαλέσει σε μερικούς το γεγονός ότι, αν κάποιο μέλος συνδέεται στο Google+ , μέσα απο το κινητό του τηλέφωνο, τότε η εταιρεία πιθανότατα συλλέγει στοιχεία όπως, τον αριθμό του κινητού τηλεφώνου, τον αριθμό του καλουμένου, αριθμούς προώθησης, την ώρα και την ημερομηνία κλήσεων ακόμη και τη διάρκεια των κλήσεων! Επιπλέον, οι υπεύθυνοι του συγκεκριμένου κοινωνικού δικτύου, πιθανότατα να καταχωρούν στα συστήματά τους πληροφορίες σχετικές τόσο με την τοποθεσία του χρήστη, όσο και με τις εφαρμογές που είτε καταργεί την εγκατάστασή τους, είτε ενημερώνονται απο καινούργιές ρυθμίσεις. Όσο αναφορά τώρα, τον τρόπο με τον οποίο η εταιρεία Google+ διαχειρίζεται τις προσωπικές πληροφορίες και δεδομένα των χρηστών, διαβεβαιώνει πως τις χρησιμοποιεί αποκλειστικά και μόνο για για την παροχή, διατήρηση και βελτίωσή υπηρεσιών και για την προστασία τόσο της ίδιας της εταιρείας, όσο και των χρηστών της. Επίσης,αναφέρει πως χρησιμοποιεί αυτά τα στοιχεία για να προσφέρει στα μέλη της προσαρμοσμένο περιεχόμενο, όπως πιο σχετικά αποτελέσματα αναζήτησης και διαφημίσεις. Ακόμη, μέσα στην πολιτική προστασίας της, η εταιρεία αναφέρει πως συλλέγει πληροφορίες μέσα απο διάφορες τεχνολογίες, όπως ετικέτες εικονοστοιχείων[8] με σκοπό να βελτιώσουν την εμπειρία του χρήστη και τη συνολική ποιότητα των υπηρεσιών τους. Για παράδειγμα, με την αποθήκευση των προτιμήσεών της γλώσσας του κάθε χρήστη-μέλος, θα μπορούν να εμφανίζουν τις υπηρεσίες τους στη γλώσσα που προτιμάνε. Παρόλαυτα, ευαίσθητες προσωπικές πληροφορίες, όπως αυτές που έχουν σχέση με τη φυλή, τη θρησκεία, τον σεξουαλικό προσανατολισμό ή δεδομένα υγείας δεν αποκαλύπτονται ποτέ. Απο την άλλη μεριά, η εταιρεία Google+ παρέχει την δυνατότητα στους χρήστες της, να παραμετροποιήσουν τις διάφορες ρυθμίσεις, έτσι ώστε να ελέγχουν με ποιο τρόπο θα εμφανίζεται το προφίλ τους και σε ποιούς. Επιπρόσθετα, οι χρήστες έχουν το δικαίωμα να ασκήσουν κριτική και έλεγχο σε συγκεκριμένους τύπους πληροφοριών, οι οποίες σχετίζονται με τον λογαριασμό τους χρησιμοποιώντας τον πίνακα ελέγχου της ίδιας της εταιρείας Google+ . Σε αυτό το σημείο, καλό θα ήταν να γίνει μία μικρή αναφορά σχετικά με τις πληροφορίες των χρηστών, τις οποίες η εταιρεία μοιράζεται.

[8] Η ετικέτα εικονοστοιχείων είναι ένας τύπος τεχνολογίας που τοποθετείται σε έναν ιστότοπο ή στο κύριο μέρος ενός μηνύματος ηλεκτρονικού ταχυδρομείου με σκοπό την παρακολούθηση της δραστηριότητας σε ιστότοπους ή κατά το άνοιγμα ή μετάβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου, και χρησιμοποιείται συχνά σε συνδυασμό με cookie.

Πρώτα απ' όλα, περιγράφει μέσα στην πολιτική απορρήτου της, πως προσωπικά στοιχεία και πληροφορίες τις παρέχουν σε τρίτους, αφού πρώτα έχει δοθεί η συναίνεση απο μεριάς των ίδιων των χρηστών. Στη συνέχεια, αναφέρουν πως ίσως μοιραστούν προσωπικά στοιχεία των χρηστών για νομικούς σκοπούς. Πιο αναλυτικά, δίνουν το δικαίωμα πρόσβασης σε τρίτους, όταν η πρόσβαση, η χρήση, η διατήρηση ή η αποκάλυψη των πληροφοριών είναι εύλογα απαραίτητη, προκειμένου να ικανοποιηθούν τυχόν ισχύοντες νόμοι, νομικές διατάξεις ή επιβλητέα αιτήματα οργανισμών, με σκοπό πάντα να εντοπίσουν, να αποτρέψουν ή να αντιμετωπίσουν απάτες σχετικές με τις διευθύνσεις και ζητήματα ασφαλείας. Συμπληρωματικά με τα προηγούμενα, τα προσωπικά δεδομένα αποκαλύπτονται, όταν υπάρχει η ανάγκη να προστατεύσουν, οι ειδικοί, από επικείμενη βλάβη τα δικαιώματα, την ιδιοκτησία ή την ασφάλεια της εταιρείας, των χρηστών της ή του κοινού, όπως επιτρέπεται από την ισχύουσα νομοθεσία. Κλείνοντας, να αναφέρουμε, πως η εταιρεία της συγκεκριμένης ιστοσελίδας κοινωνικής δικτύωσης καταβάλλει καθημερινά μεγάλες προσπάθειες προκειμένου να προστατέψει τους χρήστες-μέλη από τυχόν μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση, αποκάλυψη ή καταστροφή των στοιχείων που έχει στην κατοχή της. Μερικά παραδείγματα είναι ότι, η πρόσβαση στα προσωπικά στοιχεία περιορίζεται μόνο σε υπαλλήλους, αναδόχους και αντιπροσώπους της Google+, οι οποίοι υπόκεινται σε αυστηρές συμβατικές υποχρεώσεις εμπιστευτικότητας και ενδέχεται να υπόκεινται σε πειθαρχικές διαδικασίες ή ακόμη και σε απόλυση, εάν δεν ανταποκριθούν σε αυτές τις υποχρεώσεις. Επιπλέον, η εταιρεία κρυπτογραφεί πολλές απο της υπηρεσίες της κάνοντας χρήση SSL[9], καθώς επίσης προσφέρει και επαλήθευση σε δύο βήματα, όταν ο χρήστης μεταβαίνει στον λογαριασμό του. Τέλος, παρουσιάζεται παρακάτω ένας συγκεντρωτικός πίνακας στον οποίο φαίνονται, τόσο τα πιο δημοφιλή κοινωνικά δίκτυα, όσο και οι πρακτικές που ακολουθούν σχετικά με την πολιτική απορρήτου και την προστασία της ιδιωτικότητας.

[9] Η υπηρεσία **SSL (S**ecure **S**ockets **L**ayer**),** η οποία πλέον ονομάζεται **TLS (T**ransport **L**ayer **S**ecurity**)**, είναι το πρωτόκολλο κρυπτογράφησης που παρέχει ασφάλεια για τις επικοινωνίες μέσω δικτύων όπως το Internet. Αυτό το πρωτόκολλο είναι απαραίτητο σε ιστοσελίδες οι οποίες ανταλλάσουν σημαντικές πληροφορίες όπως προσωπικά δεδομένα ή κωδικούς πιστωτικών καρτών.

4.5 Συγκριτική παρουσίαση των μηχανισμών προστασίας της ιδιωτικότητας

Τα κοινωνικά δίκτυα αποτελούν πλέον μέρος της καθημερινότητας των χρηστών του διαδικτύου και καθημερινά οι ίδιοι ξοδεύουν αρκετό απο τον χρόνο τους για να συνδεθούν και να πλοηγηθούν σε κάποιο ή ακόμη και σε κάποια απο αυτά. Όπως όμως αναφέρθηκε και νωρίτερα, το καθένα απο τα κοινωνικά δίκτυα ακολουθεί την δική του πολιτική προστασίας, η οποία διαφέρει ανάλογα με το κοινωνικό δίκτυο, στο οποίο αναφερόμαστε. Παρακάτω υπάρχει ένας συγκεντρωτικός πίνακας, στον οποίο παρουσιάζονται περιληπτικά οι διαφορές αλλά και οι ομοιότητες των τριών πιο γνωστών κοινωνικών δικτύων το Facebook, το Twitter και το Google+ .

Χαρακτηριστικά	**Facebook**	**Twitter**	**Google+**
Ρυθμίσεις Ιδιωτικότητας	Οι ρυθμίσεις είναι ευπροσάρμοστες, δίνοντας έτσι την δυνατότητα στους χρήστες να αποφασίζουν ποιες πληροφορίες θα μοιράζονται & με ποιούς.	Οι χρήστες έχουν την δυνατότητα επιλογής μεταξύ δημόσιου(προκαθορισμένη επιλογή) ή προστατευμένου προφίλ(επικοινώνια μόνο με όσους ειναι εξουσιοδοτημένοι).	Οι ρυθμίσεις είναι ευπροσάρμοστες, δίνοντας έτσι την δυνατότητα στους χρήστες να αποφασίζουν ποιες πληροφορίες θα μοιράζονται & με ποιούς.
Ύπαρξη διαφημίσεων τρίτων κατασκευαστών	Ναι	Όχι	Ναι
Δυνατότητα αποκλεισμού ατόμων	Ναι	Ναι	Ναι
Δημιουργία λιστών/ομάδων	Ναι	Όχι	Ναι
Υποστήριξη εφαρμογών τρίτων κατασκευαστών	Ναι	Ναι	Όχι
ΕπαλήθευσηΛογαριασμών (verified accounts)	Όχι	Ναι	Ναι
Ιδιωτικές Συνομιλίες	Ναι	Όχι	Ναι (ακόμη και βίντεο)

Πίνακας (2) - Διάσημα κοινωνικά δίκτυα και σύγκριση βασικών χαρακτηριστικών

Όπως φαίνεται και στον πίνακα (2), σχετικά με τις ρυθμίσεις ιδιωτικότητας στα κοινωνικά δίκτυα Facebook και Google+ παρατηρούμε πως είναι ευπροσάρμοστες και ο χρήστης έχει πολλές επιλογές, σύμφωνα με τις οποίες μπορεί να διαμορφώσει το προσωπικό του προφίλ με πολλούς τρόπους. Αντίθετα, στο κοινωνικό δίκτυο Twitter οι ρυθμίσεις ιδιωτικότητας είναι πιο περιορισμένες, αφού ο χρήστης έχει μόνο δύο επιλογές, είτε το προφίλ του να είναι δημόσιο και ο καθένας να έχει πρόσβαση σε οποιαδήποτε δημοσίευση και φωτογραφία του, είτε κλειδωμένο και μόνο όσοι τον "ακολουθούν" να έχουν την δυνατότητα να παρατηρούν τις κινήσεις και τις δημοσιεύσεις του. Έτσι, θα λέγαμε πως τα δύο κοινωνικά δίκτυα Facebook και Google+ είναι συγκριτικά πιο ασφαλή απο το Twitter. Στη συνέχεια, παρατηρούμε ότι στα κοινωνικά δίκτυα Facebook και Google+ υπάρχουν διαφημίσεις τρίτων κατασκευαστών, σε αντίθεση με την ιστοσελίδα του δικτύου Twitter, όπου δεν υπάρχουν καθόλου διαφημίσεις. Παρόλ'αυτά, στις πολιτικές προστασίας που ακολουθούν και τα τρία κοινωνικά δίκτυα υπάρχει η αναφορά, ότι τα δεδομένα και οι πληροφορίες των χρηστών δεν πουλιούνται σε διαφημιστές χωρίς την συγκατάθεση των ίδιων. Έπειτα, παρατηρούμε ότι η δυνατότητα αποκλεισμού ατόμων υπάρχει και στα τρία κοινωνικά δίκτυα, επιτρέποντας έτσι στους χρήστες να διαλέγουν τα άτομα που μόνο αυτοί επιθυμούν. Από την άλλη μεριά, στα δύο κοινωνικά δίκτυα Facebook και Google+ υπάρχει και η δυνατότητα δημιουργίας ομάδων και λιστών, όπου μπορούν να απαρτίζονται απο συγκεκριμένα άτομα, τα οποία είτε έχουν περισσότερες δικαιοδοσίες στο προφίλ ενός χρήστη, είτε πιο περιορισμένες. Κάτι τέτοιο όμως, δεν είναι δυνατό στο Twitter. Σχετικά τώρα με την υποστήριξη εφαρμογών τρίτων κατασκευαστών, όπως διαδικτυακά παιχνίδια, ανάγνωση ειδήσεων απο άλλες ιστοσελίδες κλπ, φαίνεται πως οι ιστοσελίδες κοινωνικής δικτύωσης Facebook και Twitter το επιτρέπουν, ενώ το Google+ όχι. Στη συνέχεια, βλέπουμε την προοπτική επαλήθευσης λογαριασμού, όπου στο κοινωνικό δίκτυο Facebook είναι ανύπαρκτη, ενώ στα άλλα δύο υφίσταται. Κλείνοντας, τίθεται το θέμα της ιδιωτικής συνομιλίας, όπου στα δίκτυα Facebook και Google+ υπάρχει παρέχοντας ταυτόχρονα και την δυνατότητα συνομιλίας με χρήση βίντεο στο δεύτερο, αντίθετα απο το Twitter όπου δεν υπάρχει καμία τέτοια επιλογή.

Κεφάλαιο 5: Προτάσεις αποτελεσματικής προστασίας της ιδιωτικότητας

5.1 Προτάσεις προς τα κοινωνικά δίκτυα

Στο προηγούμενο κεφάλαιο περιγράφηκε λεπτομερώς, πως τα κοινωνικά δίκτυα απο την μεριά τους βοηθούν τους χρήστες στην προσπάθεια προστασίας της ιδιωτικότητάς τους. Οι ιστοσελίδες κοινωνικής δικτύωσης, μέσα από την πολιτική απορρήτου, την οποία δημοσιεύουν και υπάρχει πάντοτε διαθέσιμη στο διαδίκτυο, διαχωρίζουν την θέση τους και κάνουν ξεκάθαρη την στάση τους στο πως αντιμετωπίζουν, αλλά και χειρίζονται θέματα ιδιωτικότητας των χρηστών. Σ' αυτό το σημείο, καλό θα ήταν να προτείνουμε κάποιες επιπλέον αρχές, τις οποίες οι ιστοσελίδες κοινωνικής δικτύωσης θα μπορούσαν να υιοθετήσουν, ενισχύοντας κατά αυτόν τον τρόπο την ιδιωτικότητα των χρηστών. Έστω για παράδειγμα, πως έχουμε ένα κοινωνικό δίκτυο, ποιά θα ήταν τα δέκα βασικά σημεία που θα οφείλαμε να προσέξουμε, αλλά και να υιοθετήσουμε, έτσι ώστε να διαφυλάξουμε, όσο καλύτερα γίνεται την ιδιωτικότητα των χρηστών μας; Παρακάτω, παρουσιάζονται καθοδηγήσεις και συμβουλές προς ένα κοινωνικό δίκτυο :

- Αποφυγή διαφημίσεων τρίτων κατασκευαστών στις ιστοσελίδες κοινωνικής δικτύωσης.
- Να ζητείται επαλήθευση λογαριασμών των χρηστών, έτσι ώστε οι χρήστες να αισθάνονται περισσότερη ασφάλεια.
- Προσαρμογή των ρυθμίσεων του δικτύου, έτσι ώστε να περιορίζεται η πρόσβαση και τα δικαιώματα των των υπολοίπων χρηστών του δικτύου στο προφίλ του εκάστοτε χρήστη.
- Απόκρυψη πληροφοριών και δεδομένων των χρηστών - μελών του κοινωνικού δικτύου απο τα αποτελέσματα των μηχανών αναζήτησης.

- Σύνταξη πολιτικής απορρήτου περιορισμένης έκτασης, με ευνόητους και κατανοητούς όρους, καθώς επίσης να περιέχεται και μία ποικιλία απο σαφή παραδείγματα.
- Να παρέχεται ένας διαδικτυακός οδηγός, ο οποίος θα συμβουλεύει τους χρήστες, πως θα προστατευτούν στο έπακρο και με ποιόν τρόπο, βάσει βημάτων, που θα παραμετροποιούν τις ρυθμίσεις που επιθυμούν.
- Επιβολή τακτικών αλλαγών των κωδικών πρόσβασης, με στόχο την αποφυγή παραβίασής τους απο κακόβουλα προγράμματα υπολογιστών.
- Απόκρυψη και σε καμία περίπτωση πώληση προσωπικών δεδομένων και πληροφοριών των χρηστών σε τρίτους, παραμόνο σε περιπτώσεις όπου κριθεί απαραίτητο απο την δικαιοσύνη.
- Δεν θα επιτρεπόταν η επισήμανση άλλων χρηστών σε φωτογραφίες και δημοσιεύσεις, χωρίς πρώτα να υπάρχει η συγκατάθεσή τους.
- Θα επιτρεπόταν η πλήρης διαγραφή ενός προφίλ - λογαριασμού, χωρίς να υπήρχαν αντίγραφα ασφαλείας στην βάση δεδομένων του δικτύου.

Σύμφωνα, λοιπόν με την εφαρμογή των παραπάνω δέκα βημάτων από την μεριά ενός κοινωνικού δικτύου, πιστεύουμε πως η διαφύλαξη της ιδιωτικότητας των χρηστών μπορεί να στεφθεί με επιτυχία.

5.2 Προτάσεις προς τους χρήστες

Προηγουμένως, αναφέρθηκαν κάποιες προτάσεις, οι οποίες απευθύνονται προς τα κοινωνικά δίκτυα, στοχεύοντας έτσι στην καλύτερη προστασία της ιδιωτικότητας των χρηστών - μελών τους. Σε αυτό το σημείο όμως, αποτελεσματικό θα ήταν, εάν γινόταν και μια μικρή αναφορά με περαιτέρω προτάσεις και συμβουλές προς τους χρήστες. Επομένως, αν ένας χρήστης επιθυμεί να πλοηγηθεί μέσα σε μια ιστοσελίδα κοινωνικής δικτύωσης με ασφάλεια, καλό θα ήταν να ακολουθήσει τα παρακάτω βήματα :

- Να διαβάζει προσεχτικά τους όρους της πολιτικής απορρήτου και να τους κατανοήσει πλήρως, προτού συμφωνήσει με αυτούς.
- Να είναι ιδιαίτερα προσεχτικός με το περιεχόμενο του φωτογραφικού υλικού, που πρόκειται να δημοσιοποιήσει, αφού όπως έχει αναφερθεί και προηγουμένως, πολλές είναι ο πληροφορίες που μία φωτογραφία δύναται να αποκαλύψει.
- Ιδιαίτερα αποδοτικό θα ήταν, εάν ο χρήστης δεν αποδεχόταν αιτήματα φιλίας απο άτομα τα οποία δεν γνωρίζει καθόλου.
- Χρήσιμο θα ήταν, αν ο εκάστοτε χρήστης κοινοποιούσε μόνο όσες προσωπικές πληροφορίες είναι απαραίτητες και μόνον αυτές.
- Καλό επίσης θα ήταν, ο χρήστης να μην επισημαίνει γεωγραφικές τοποθεσίες στις οποίες παρευρίσκεται και να μην επιτρέπει ούτε στους φίλους του να πραγματοποιούν την συγκεκριμένη ενέργεια για λογαριασμό του.
- Να διατηρεί το προφίλ του κρυφό απο το ευρύ κοινό και να έχουν πρόσβαση μόνο οι φίλοι και οι γνωστοί του.
- Να μην επιτρέπει την επισήμανση του εαυτού τόσο στις φωτογραφίες του, όσο και στις φωτογραφίες των φίλων του.
- Να μην κοινοποιεί τον αριθμό του κινητού του τηλεφώνου, κάτι το οποίο συχνά ζητείται, αλλά φυσικά είναι προαιρετικό.
- Να είναι επιφυλαχτικός και να διαβάζει προσεχτικά τους όρους αποδοχής, προτού κάνει χρήση εφαρμογών τρίτων κατασκευαστών.
- Να μην αποθηκεύει τον κωδικό πρόσβασής του, απο όποια συσκευή και αν συνδέεται στο κοινωνικό δίκτυο.

Επομένως, αν ο οποιοσδήποτε χρήστης ακολουθήσει πιστά τα προηγούμενα βήματα, μπορεί να αισθάνεται ασφάλεια και σιγουριά για το προσωπικό του προφίλ και τα δεδομένα που δημοσιεύει. Η χρήση και η πλοήγηση μέσα στα κοινωνικά δίκτυα ποτέ δεν ήταν απαγορευτική και ιδιαίτερα επικίνδυνη, αρκεί να πραγματοποιείται πάντοτε με τις απαραίτητες προφυλάξεις.

Κεφάλαιο 6 : Συμπεράσματα - Επεκτάσεις

6.1 Συμπεράσματα

Τα διαδικτυακά κοινωνικά δίκτυα αποτελούν ένα εξαιρετικό φαινόμενο στις μέρες μας. Ποτέ άλλοτε τόσοι πολλοί άνθρωποι δεν είχαν την ευκαιρία να έρθουν σε επαφή, να συνομιλήσουν, να ανταλλάξουν φωτογραφίες και ιδέες και γενικότερα να επικοινωνούν με τόση μεγάλη ταχύτητα και με τόσο μικρό κόστος. Η διάδοση των κοινωνικών δικτύων πραγματοποιήθηκε με ραγδαίο ρυθμό ανάπτυξης, αφού τα πλεονεκτήματα που τα συνόδευαν ήταν πρωτοποριακά και πολλά παραπάνω απο τα αναμενόμενα. Παρόλ'αυτα, δημιουργήθηκαν και πολλές αντιδράσεις στον αντίποδα, αφού οι συνέπειες ήταν αναπόφευκτες. Στην εργασία αυτή, παρουσιάστηκαν κυρίως οι κίνδυνοι και οι απειλές γύρω απο την ιδιωτικότητα των χρηστών, καθώς επίσης και οι πολιτικές προστασίας που ακολουθούν τα πιο γνωστά κοινωνικά δίκτυα. Από τα πρώτα συμπεράσματα στα οποία καταλήγουμε είναι, ότι οι πολιτικές ιδιωτικότητας των ιστοτόπων αυτών δεν συναντούν ιδιαίτερη αποδοχή απο τους ίδιους τους χρήστες. Η πλειοψηφία των χρηστών αδιαφορεί παντελώς γι' αυτές, αφού τις θεωρεί κουραστικές, με δυσνόητους νομικούς όρους και ιδιαίτερα εκτενείς, με αποτέλεσμα να παραμένει στην άγνοια και συχνά να πέφτει θύμα παραβίασης της ιδιωτικότητάς του. Ωστόσο, στην παρούσα εργασία, αλλά και στο διαδίκτυο υπάρχουν πληθώρα προτάσεων και συμβουλών, έτσι ώστε οι χρήστες να ενημερώνονται και να πετυχαίνουν μια πιο ορθή χρήση των ιστοσελίδων αυτών. Η ενημέρωση, όπως και η παρακολούθηση των εξελίξεων στα θέματα ιδιωτικότητας παίζει το πιο σημαντικό ρόλο και όλοι οι χρήστες ανεξαιρέτως θα πρέπει να είναι σε επαγρύπνηση. Η τεχνολογία δημιουργήθηκε απο τον άνθρωπο και ο άνθρωπος είναι αυτός που μπορεί να την καθορίσει. Η κοινωνικότητα είναι στη φύση του ανθρώπου και κανείς δεν μπορεί να την περιορίσει. Αξίζει να αξιοποιήσουμε τα θετικά που προσφέρει και να περιορίσουμε τις αρνητικές συνέπειες (Άννα Λιούπα, 2011).

6.2 Επεκτάσεις

Τα κοινωνικά δίκτυα βρίσκονται ακόμη στην αρχή της ανάπτυξης τους και μέσα στα επόμενα χρόνια η εξέλιξή τους θα είναι ακόμη μεγαλύτερη. Αυτό θα έχει ως αποτέλεσμα, οι ανησυχίες των χρηστών σχετικά με την προστασία της ιδιωτικότητάς τους και να αυξηθούν, αλλά και να γίνουν εντονότερες. Φυσιολογικό επακόλουθο λοιπόν και σχεδόν απαραίτητο θα είναι, να πραγματοποιηθεί μελλοντικά περαιτέρω έρευνα και ανάλυση γύρω απο το θέμα της ιδιωτικότητας των χρηστών. Στην εργασία αυτή παρουσιάστηκαν οι βασικοί κίνδυνοι και απειλές κατά της ιδιωτικότητας στα κοινωνικά δίκτυα, που υφίστανται αυτήν την περιόδο στον κόσμο του διαδικτύου. Όμως, οι κίνδυνοι που παραμονεύουν μέσα σε ένα κοινωνικό δίκτυο δεν περιορίζονται μόνο σ' αυτούς που αφορούν την ιδιωτικότητα των χρηστών - μελών. Επομένως, σε μία μελλοντική έρευνα, καλό θα ήταν να παρουσιαστούν και να αναλυθούν και κίνδυνοι και απειλές διαφορετικής φύσεως, αφού στην παρούσα πτυχιακή εργασία η αναφορά σ' αυτούς είναι ιδιαίτερα περιορισμένη. Ωστόσο, με την αστραπιαία εξέλιξη τόσο του διαδικτύου, όσο και των κοινωνικών ιστοτόπων δεν αποκλείεται να εμφανιστούν νέοι και πιο απειλητικοί κίνδυνοι, οι οποίοι με την σειρά τους θα κέντριζαν το ενδιαφέρον αναγνωστών, εάν κάποιος τους συμπεριελάμβανε σε μία έρευνα. Στη συνέχεια, και καθώς η εργασία προχωράει, συναντάμε πιθανές προτάσεις και συστάσεις προς τους χρήστες, που σκοπό έχουν να βοηθήσουν τους τελευταίους να ενισχύσουν την προστασία τους. Παρόλ'αυτα, είναι σχεδόν αναγκαίο να προταθούν και να ερευνηθούν επιπλέον προτάσεις και καθοδηγήσεις σε κάποια μελλοντική εργασία. Επίσης, στην παρούσα πτυχιακή εργασία, παρουσιάστηκαν και αναλύθηκαν οι πολιτικές προστασίας τριών απο των πιο γνωστών κοινωνικών δικτύων των ημερών μας. Με το πέρασμα όμως των καιρών, οι ιστοσελίδες κοινωνικής δικτύωσης αλλάζουν τις πολιτικές απορρήτου και τις τροποποιούν σύμφωνα με το δικό τους συμφέρον. Επομένως, η ενότητα που αναλύει τις πολιτικές των τριών κοινωνικών δικτύων, είναι δεδομένο πως χρήζει μεγαλύτερης διερεύνησης. Στο μέλλον όμως, θα εμφανιστούν σίγουρα και άλλα καινούργια, τα οποία σίγουρα θα αποτελέσουν αντικείμενο εκτεταμένης έρευνας. Επιπρόσθετα, στην παρούσα πτυχιακή εργασία θα μπορούσε να προστεθεί και μία στατιστική έρευνα, που θα ήταν δυνατόν να πραγματοποιηθεί διαδικτυακά (online). Η στατιστική αυτή έρευνα θα απευθυνόταν σε χρήστες του διαδικτύου και ειδικότερα σε όλους εκείνους που

διατηρούν λογαριασμό σε κάποιο κοινωνικό δίκτυο. Οι ερωτήσεις θα μπορούσαν να αφορούν το πόσο καλά χειρίζεται ο χρήστης την ιδιωτικότητά του, εάν γνωρίζει το βαθμό επικινδυνότητας ή ακόμη και το πως το κάθε μέλος ενός τέτοιου δικτύου έχει πέσει θύμα απάτης και εκμετάλλευσης. Με μια τέτοια έρευνα, η εργασία θα γινόταν ακόμη πιο ενδιαφέρουσα, αφού εκτός απο το θεωρητικό κομμάτι, θα παρατηρούσαμε τις συνέπειες και στην πράξη. Ακόμη, μία ακόμη πρόταση για μελλοντική έρευνα, θα μπορούσε να είναι και η επανάληψη της παρούσας έρευνας εμπλουτισμένης με νομοθετικές διατάξεις και πλαίσια, που θα ισχύσουν ή ισχύουν ήδη σχετικά με τα δικαιώματα των χρηστών περί ιδιωτικότητας. Δυστυχώς, σε χώρες οι οποίες είναι αναπτυσσόμενες, αλλά και σε άλλες που είναι υποανάπτυχτες η ενασχόληση με τις ιστοσελίδες κοινωνικής δικτύωσης δεν απουσιάζει. Αυτό έχει ως αποτέλεσμα, να μην υπάρχουν οι αναγκαίες νομοθετικές διατάξεις οι οποίες θα μεριμνήσουν για την προστασία της ιδιωτικότητας των χρηστών και των προσωπικών τους δεδομένων. Έτσι, οι συγκεκριμένοι πολίτες συνδέονται στα διάφορα κοινωνικά δίκτυα, δίχως καμία ενημέρωση και εκπαίδευση και κατά συνέπεια δίχως καμία προφύλαξη. Το γεγονός αυτό, θα μπορούσε να αποτελέσει αντικείμενο σε μια μελλοντική επέκταση της παρούσας πτυχιακής εργασίας.

ΑΝΑΦΟΡΕΣ

Παπαβασιλείου, Ραπτοπούλου, (2011), "Τεχνολογίες κοινωνικής δικτύωσης στην εκπαίδευση", Ελλάδα

Παπανικολάου Ελένη, (2011), "Συλλογή, αξιοποίηση και επεξεργασία πληροφοριών που παρέχουν τα κοινωνικά δίκτυα για υποστήριξη εφαρμογών που τρέχουν σε περιβάλλοντα κοινωνικών δικτύων (Facebook)", Ελλάδα, Πάτρα

Παπαπαύλου Παύλος, (2012), "432 εκ. ενεργοί χρήστες στο Facebook", http://www.enternity.gr, Ελλάδα

Πάσσας, Ισίδωρος, (2009), Κοινωνικά Δίκτυα στο Internet. Η νέα πρόκληση στην κοινωνία για την νέα γενιά.

Ben, S. I., and G. F. Gauss, eds, (1983*)*, Public and *Private* in Social Life, New York: St.

Bloustein, E., (1964), "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", *New York University Law Review* 39:962-1007

Franchise Success Team, (2011), Franchise Portal.gr, InNews, Greece

Fried, Charles.,(1969), "Privacy" in *Law, Reason, and Justice: Essays in Legal Philosophy* (Graham B. J. Hughes ed., New York University Press).

Gerstein, R., (1978), "Intimacy and Privacy", *Ethics* 89: 76-81

James RachelsSource, (Summer, 1975), Philosophy and Public Affairs, Vol. 4, No. 4

Robin Ian MacDonald Dunbar, (2011), "Internet Communities", University of Oxford

Rodica Tirtea, (2011), Enisa, "Privacy in online Services" , Portugal, Lisbon

ΒΙΒΛΙΟΓΡΑΦΙΑ

- "US & EU Authorities Review Privacy Threats on social Networking Sites", Tracy Gray, Zeggane Maxwell, Hogan & Harston Boulder, (2008), France, Paris
- http://www.pi.ac.cy/InternetSafety/kindinoi_parabiidiotik.html
- "Security issues and recommendations for online social networks", Hogben Giles, (2007), Enisa,
- http://translate.google.gr/translate?hl=el&langpair=en|el&u=http://www.aksindiblog.com/2010/05/social-media-privacy-known-threats-and.html
- http://www.pcworld.com/article/196787/goodbye_to_privacy.html
- http://www.google.com/intl/el/policies/privacy/
- http://www.google.com/intl/el/policies/terms/
- http://www.facebook.com/note.php?note_id=%20322194465300
- http://www.e-innovator.gr/ssl/ssl.php
- http://thesocialmediaguide.com/social_media/social-media-comparison-charts
- http://www.pcmag.com/article2/0,2817,2388307,00.asp
- http://socialcompare.com/en/comparison/google-plus-vs-facebook-vs-twitter-comparison-table
- http://blog.tweetsmarter.com/wp-content/uploads/2011/07/social.medial-comparison.png
- http://socialtimes.com/google-plus-facebook-privacy_b79772
- http://ec.europa.eu/justice/data-protection/data-collection/index_en.htm

Field Code Changed

Field Code Changed

Field Code Changed

- http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm#359
- http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf
- http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- http://ec.europa.eu/justice/data-protection/index_el.htm
- http://nemertes.lis.upatras.gr/
- http://online.wsj.com/article/SB122170459104151023.html?mod=googlenews_wsj
- http://networkconference.netstudies.org/2012/social-networking-sites-more-popular-more-harm/
- hτtp://us.mcafee.com/en-us/local/docs/SocialNetworkinge-guide.pdf
- http://www.facebook.com/press/info.php?statistics
- http://www.checkfacebook.com/
- http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/
- http://www.slideshare.net/EmergenceMedia/facebook-demographics-user-statistics-emergence-media
- http://www.internetworldstats.com/facebook.htm
- http://www.socialbakers.com/facebook-statistics/greece
- http://books.google.com/books?hl=el&lr=&id=SE2iRgeYYwcC&oi=fnd&pg=PR5&dq=%E2%80%9CPRIVACY+IN+SOCIAL+NETWORKS:+A+SURVEY%E2%80%9D,+from+the+book+%E2%80%9CSOCIAL+NETWORK+DATA+ANALYTICS%E2%80%9D

&ots=lHdNNtVVPt&sig=SIJEpY47Lq790cnkjfsU5dYzHfc#v=onepage&q&f=false

- http://www.fastcompany.com/articles/2008/10/social-networking-security.html
- http://learn20.wikispaces.com/%CE%A5%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%AF%CE%B5%CF%82+%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CF%8E%CE%BD+%CE%94%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD
- http://www.epixeiro.gr/index.php?option=com_content&view=article&id=1083:2011-10-11-14-43-09&catid=66:2010-07-21-22-27-20&Itemid=257
- http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf
- http://en.wikipedia.org/wiki/CBIR
- http://www.enternity.gr/Article/432-εκ.-ενεργοί-χρήστες-στο-Facebook/7620.html