Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας για την υποστήριξη Υπηρεσιών Κοινωνικών Δικτύων (Privacy Enhancing Technologies for supporting Social Networking Services)

Αθανασία Βλάχου

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Σεπτέμβριος 2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας για την υποστήριξη Υπηρεσιών Κοινωνικών Δικτύων (Privacy Enhancing Technologies for supporting Social Networking Services)

Αθανασία Βλάχου

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Σεπτέμβριος 2014

Περίληψη

Στη σημερινή κοινωνία, χρησιμοποιείται ευρύτατα το διαδίκτυο και οι υπηρεσίες κοινωνικής δικτύωσης. Πρόσφατες μελέτες αναδεικνύουν , ως ένα από τα σημαντικότερα θέματα που απασχολούν τους χρήστες των υπηρεσιών κοινωνικών δικτύων , το θέμα της Ιδιωτικότητας. Στόχος της παρούσας μεταπτυχιακής διατριβής είναι να παρουσιάσει το πρόβλημα και να προτείνει βέλτιστες πρακτικές προστασίας.

Αρχικά θα μελετήσουμε την έννοια της Ιδιωτικότητας και το πώς αυτή ορίζεται νομικά, το νομικό πλαίσιο που υπάρχει στον κόσμο, στην Ευρώπη και στην Ελλάδα. Ακολούθως θα αναφερθούμε στα τρία πιο δημοφιλή δίκτυα κοινωνικής δικτύωσης, Facebook, Google+, Twitter, τα οποία και θα μελετήσουμε.

Στη συνέχεια, θα αναφερθούμε στα πιο σημαντικά είδη τεχνολογιών ενίσχυσης της Ιδιωτικότητας (PETs), που προστατεύουν όχι μόνο στο κομμάτι της χρήσης των δικτύων κοινωνικής δικτύωσης, αλλά την πλοήγηση στο διαδίκτυο και την ανταλλαγή αρχείων. Η χρήση των PETs ελαχιστοποιεί τη συλλογή και τη χρήση προσωπικών δεδομένων από διάφορους φορείς και οργανισμούς .

Τα δίκτυα κοινωνικής δικτύωσης (SNS), παρέχουν στους χρήστες δυνατότητα ρύθμισης του απορρήτου τους και θα αναλύσουμε πως μπορούμε να το πετύχουμε αυτό, σε κάθε ένα από τα τρία δίκτυα κοινωνικής δικτύωσης που μελετούμε.

Ακολούθως, θα αναφερθούμε σε προτεινόμενες αρχιτεκτονικές δικτύων κοινωνικής δικτύωσης, οι οποίες λαμβάνουν στο σχεδιασμό και τη δομή τους την προστασία των προσωπικών δεδομένων.

Τέλος θα γίνει μια βιβλιογραφική ανασκόπηση για το βαθμό διείσδυσης των τεχνολογιών ενίσχυσης της Ιδιωτικότητας (PETs) στα μέσα κοινωνικής δικτύωσης (SNS) και τους παράγοντες που αντιτίθενται στη διαδικασία αυτή.

Summary

In today's society widely used internet and social networking services. Recent studies reveal, as one of the major concerns of the users of social network services, the issue of privacy. The aim of this work is to present the problem and propose optimal protection practices.

We will first study the concept of privacy and how it is defined legally, the legal framework that exists in the world, in Europe and in Greece. Then we will refer to the three most popular social networks, Facebook, Google+, and Twitter, which we will study.

Then we will refer to the most important types of the privacy enhancing technologies (PETs), which protect not only track the use of social networks, but the web browsing and file sharing. The use of PETs minimizes the collect and use of personal data by various agencies and organizations.

The social networks (SNS) provide users configurable privacy and will analyze how we can achieve this, each of the three social networks that we study.

Subsequently, we will refer to proposed social media network architectures that take the design and structure of the protection of personal data.

Finally we made a literature review on the penetration of privacy enhancing technologies (PETs) in social media (SNS) and the factors that oppose this process.

Ευχαριστίες

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στα πλαίσια των σπουδών μου, για την απόκτηση του Μεταπτυχιακού Διπλώματος που απονέμει το πρόγραμμα Μεταπτυχιακών Σπουδών : « Πληροφοριακά και Επικοινωνιακά Συστήματα».

Θα ήθελα να εκφράσω τις ευχαριστίες μου, προς το μέλος της εξεταστικής επιτροπής και επιβλέπων καθηγητή μου κ. Στέφανο Γκρίτζαλη για την πολύτιμη βοήθειά του καθ' όλη τη διάρκεια εκπόνησης της διπλωματικής εργασίας αλλά και για τη γενικότερη στήριξη που μου προσέφερε, καθώς θα ήταν αδύνατη η ολοκλήρωση των σπουδών μου χωρίς τη συμβολή του. Δεν θα μπορούσα να μην ευχαριστήσω και όλους τους καθηγητές, με τους οποίους συνεργάστηκα στις θεματικές ενότητες που παρακολούθησα αυτά τα τρία χρόνια των σπουδών μου, για τις γνώσεις που μου πρόσφεραν και τους ορίζοντες που μου άνοιξαν.

Τέλος, θα ήθελα να ευχαριστήσω το σύζυγό μου για την αμέριστη συμπαράστασή του, το κουράγιο, τη δύναμη που μου έδινε όλα αυτά τα χρόνια για να συνεχίσω και να πετύχω τους στόχους μου.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Τα δίκτυα κοινωνικής δικτύωσης έχουν γίνει από τους πιο δημοφιλείς στους χρήστες τρόπους για να επικοινωνούν με την οικογένεια, τους φίλους και τους συναδέλφους από οποιοδήποτε μέρος του κόσμου και αν βρίσκονται. Και ενώ υπάρχουν σημαντικά οφέλη από την υπεύθυνη χρήση των δικτύων κοινωνικής δικτύωσης, υπάρχουν και ανησυχίες σχετικά με την ασφάλεια των πληροφοριών και την προστασία της ιδιωτικής ζωής.

Ο όγκος και η προσβασιμότητα των προσωπικών πληροφοριών που διατίθενται στις ιστοσελίδες κοινωνικής δικτύωσης έχουν προσελκύσει κακόβουλα άτομα που επιδιώκουν να εκμεταλλευτούν αυτές τις πληροφορίες. Αυτός είναι ο λόγος που κάνει όλο και πιο επιτακτική την χρήση τεχνολογιών προστασίας τις Ιδιωτικότητας (PETs- Privacy Enhancing Technologies) όχι μόνο σε συνδυασμό με τα υπάρχοντα δίκτυα κοινωνικής δικτύωσης αλλά και την εφαρμογή τους στο σχεδιασμό των δικτύων της επόμενης γενιάς.

Στην παρούσα μεταπτυχιακή διατριβή θα αναφερθούμε αρχικά στην έννοια της Ιδιωτικότητας και το πώς αυτή ορίζεται νομικά, το τι νομικό πλαίσιο υπάρχει στον κόσμο, στην Ευρώπη και στην Ελλάδα. Ακολούθως θα αναφερθούμε στα πιο σημαντικά δίκτυα κοινωνικής δικτύωσης και στις τεχνολογίες προστασίας της Ιδιωτικότητας και κατά πόσο τα σύγχρονα δίκτυα έχουν

υιοθετήσει πρακτικές προστασίας των προσωπικών δεδομένων και αν υπάρχουν δίκτυα τα οποία έχουν σχεδιαστεί με βάση τις αρχές προστασίας της Ιδιωτικότητας.

Καθώς οδηγούμαστε σε μία κοινωνία όπου η συντριπτική πλειοψηφία των ανθρώπων είναι συνδεδεμένοι σε ένα ή και περισσότερα δίκτυα κοινωνικής δικτύωσης και η ενασχόλησή τους ξεκινά από πολύ μικρή ηλικία, η προστασία της Ιδιωτικότητας και των προσωπικών δεδομένων θα αρχίσει να αποτελεί μείζον θέμα .

Κεφάλαιο 2
Ιδιωτικότητα

Η ιδιωτικότητα είναι μία έννοια που πιο εύκολα περιγράφεται παρά ορίζεται. Όταν αναφερόμαστε στην ιδιωτικότητα είναι επίσης βέβαιο ότι είναι ευχερέστερο να την υπερασπίζεται κανείς ως αίτημα παρά να την ορίζει. Η παραπομπή στην περίφημη συνηγορία των Αμερικανών δικαστών Warren και Brandeis (1896) υπέρ του δικαιώματος του ατόμου σε μία ανενόχλητη ζωή (the right to be let alone) [22] είναι τόσο συνήθης όσο και, πλέον, ανεπαρκής για τον ορισμό ή ακριβέστερα τον προσδιορισμό της Ιδιωτικότητας.

Εκατό και πλέον χρόνια μετά και υπό την καταλυτική επίδραση της τεχνολογικής επανάστασης, η αντίληψη της Ιδιωτικότητας έχει σημαντικά εμπλουτιστεί με επιμέρους δικαιώματα, όπως το δικαίωμα σε ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο (ή άσυλο της κατοικίας), η προσδοκία της εχεμύθειας και φυσικά το ιδιωτικό απόρρητο των προσωπικών δεδομένων [27].

2.1 Πληροφοριακή ιδιωτικότητα

Με την πάροδο του χρόνου, αναμφίβολα και υπό την επίδραση της εξέλιξης των νέων τεχνολογιών, γινόταν όλο και περισσότερο κατανοητό ότι η ιδιωτικότητα ως αξίωση σεβασμού της απόσυρσης ή του απορρήτου παρέχει αναγκαία μεν ανεπαρκή ωστόσο προστασία στο άτομο [06]. Η διεύρυνση του προστατευτέου αγαθού αλλά και η αναγκαιότητα της κανονιστικής αντιμετώπισης των προσβολών της Ιδιωτικότητας πρόβαλαν επιτακτικότερες, όταν κατέστη αντιληπτή η ποιοτική διάφορα στις δυνατότητες συλλογής, επεξεργασίας, διάχυσης, συσχετισμού των πληροφοριών που δημιουργούσαν τα πληροφοριακά και επικοινωνιακά συστήματα και κυρίως η δυνατότητα χρήσης, ανταλλαγής και συσχετισμού των δεδομένων που έχουν συλλεχθεί για πολλαπλούς και διαφορετικούς από τους αρχικούς σκοπούς.

Η τεχνολογική δυνατότητα διείσδυσης στη ζωή και στην επικοινωνία, στην προσωπικότητα και στις συνήθειες του χρηστή ανέδειξε την ποιοτική διάσταση των κινδύνων που συνδέοντα με την αναδυόμενη Κοινωνία της Πληροφορίας, καθώς ήδη η ποσοτική αύξηση συνεπέφερε την αύξηση της έντασης, του βαθμού προσβολής των δικαιωμάτων.

Κατέστη επίσης προφανές ότι η γεωμετρική αύξηση των δυνατοτήτων επεξεργασίας της προσωπικής πληροφορίας τελούσε σε σχέση αντιστρόφως ανάλογη προς την ικανότητα του προσώπου να έχει εποπτεία της χρήσης των πληροφοριών που το αφορούν. Το διακυβευόμενο αγαθό δεν εντοπίζεται πλέον στην προστασία της αξίωσης για ανενόχλητη ιδιωτική σφαίρα αλλά αφορά στην άσκηση ελέγχου επί των ιδίων, προσωπικών πληροφοριών.

Σύμφωνα μάλιστα με τον «κλασικό» ορισμό του Westin [33], η ίδια η έννοια της Ιδιωτικότητας προσδιορίζεται ακριβώς ως η αξίωση των ατόμων, των ομάδων ή των θεσμών να προσδιορίζουν οι ίδιοι πότε, πώς και σε ποια έκταση οι πληροφορίες που τους αφορούν θα γίνονται γνωστές σε τρίτους [16].

Το γερμανικό Ομοσπονδιακό Συνταγματικό Δικαστήριο, διατυπώνοντας το δικαίωμα του πληροφοριακού αυτοπροσδιορισμού, εξαρτούσε την ανάπτυξη της προσωπικότητας στην κοινωνική συναναστροφή, στη διαμόρφωση ίδιας γνώμης, στην ελευθερία απόφασης και στη συμμετοχή στον κοινωνικό και πολιτικό διάλογο από την ελευθερία του πολίτη να (συμ)προσδιορίζει ποιες πληροφορίες που τον αφορούν θα καταστούν γνωστές στο περιβάλλον

του και αφετέρου τη δυνατότητα να εποπτεύει τον πληροφοριακό και αξιολογικό ορίζοντα αυτών με τους οποίους έρχεται σε επικοινωνία. Η προστασία των επιλογών ζωής έναντι του δημόσιου ελέγχου, σχετίζεται περαιτέρω με την ισότητα καθώς προστατεύει τα άτομα έναντι της κοινωνικής δυσμένειας ή των διακρίσεων που μπορεί να συνεπάγεται η συχνά μη εξουσιοδοτημένη γνώση μιας πληροφορίας, όπως επισημαίνεται στο Προοίμιο (αρ.25) της Σύμβασης 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα (1981).

Στην ικανότητα των ατόμων για ελεύθερες αποφάσεις και επιλογές, χωρίς παρεμβάσεις, καταγραφή και έλεγχο, βασίζει τη λειτουργία της μια κοινωνία ελευθερίας. Η ελευθερία της απόφασης δεν είναι σημαντική μόνο σε συνάρτηση με το άτομο, δε συνιστά απλώς μέσο για την πραγμάτωση των αντιλήψεων και των στόχων του σύμφωνα με τις αντιλήψεις του. Η πληροφοριακή ιδιωτικότητα αποσκοπεί στο να καταστήσει δυνατή στο άτομο μία συγκεκριμένη συμμετοχή στις διαδικασίες της κοινωνίας. Καθιστά ταυτόχρονα δυνατή την άσκηση άλλων ελευθεριών και την απόλαυση άλλων ατομικών δικαιωμάτων, όπως η ελευθερία της έκφρασης, η συμμετοχή σε πολιτικές ή συνδικαλιστικές ενώσεις και η θρησκευτική ελευθερία.

2.2 Προστασία προσωπικών δεδομένων

Η αναγκαιότητα της προστασίας της Ιδιωτικότητας προβάλλετε εντονότερα, όταν γίνεται αντιληπτή η ποσοτική και ποιοτική διαφορά στις δυνατότητες συλλογής και επεξεργασίας πληροφοριών που επιτρέπουν τα πληροφοριακά συστήματα, η οποία καθιστά δυνατή την πολυλειτουργική χρήση και την «αποξένωση» της πληροφορίας από το φορέα της, το αρχικό περιβάλλον και τους αρχικούς σκοπούς της, της μη εξουσιοδοτημένης συλλογής και επεξεργασίας της. Η σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών, η αποκέντρωση της επεξεργασίας, η διείσδυση της επεξεργασίας και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας, αλλάζουν ριζικά το περιβάλλον χρήσης της προσωπικής πληροφορίας αλλά και τα ζητήματα που εγείρονται σε σχέση με την προστασία της.

Σε αυτό το πλαίσιο διαμορφώνεται το αίτημα για προστασία προσωπικών δεδομένων. Σε αντίθεση με την ιδιωτικότητα, η προστασία προσωπικών δεδομένων εγείρεται ως αίτημα αναπόσπαστα συνδεδεμένο με την τεχνολογική εξέλιξη, καθώς αξιολογείται πως οι υφιστάμενες ρυθμίσεις δεν προσφέρουν επαρκή προστατευτική ασπίδα έναντι των διαφαινόμενων κινδύνων.

Λαμβάνοντας υπόψη τις ιδιαίτερες δυνατότητες και επιπτώσεις της ηλεκτρονικής επεξεργασίας προσωπικής πληροφορίας, η προστασία προσωπικών δεδομένων δεν περιορίζεται στη ρύθμιση και στην προστασία της πληροφορίας που το άτομο θεωρεί ιδιωτική και ευαίσθητη και για το λόγο αυτό επιθυμεί να απαγορεύσει ή να περιορίσει τη συλλογή, τη χρήση και τη διάδοσή της. Αφορά κάθε πληροφορία που αναφέρεται σε ένα φυσικό πρόσωπο, καθώς η πληροφοριακή αξία ακόμη και μιας κατ' αρχάς «αβλαβούς» πληροφορίας καθορίζεται εν τέλει από την επεξεργασία της, τον συνδυασμό της με άλλες πληροφορίες, από το περιβάλλον εντός του οποίου χρησιμοποιείται και αξιολογείται. Η προστασία των προσωπικών δεδομένων υπερβαίνει τη διάκριση μεταξύ ιδιωτικής και δημόσιας σφαίρας, καθώς κατ' αρχάς δε διακρίνει ανάμεσα σε «απλές» και «ιδιωτικές/ απόρρητες» πληροφορίες.

2.2.1 Το κανονιστικό περιβάλλον στην Ευρώπη

Στην Ευρώπη, τόσο σε εθνικό όσο και σε υπερεθνικό επίπεδο, καταγράφονται οι πρώτες δεσμευτικές κανονιστικές ρυθμίσεις για την προστασία προσωπικών δεδομένων. Τα νομοθετικά κείμενα της πρώτης γενιάς, δηλαδή της δεκαετίας του '70, που απαντώνται στα σκανδιναβικά κράτη καθώς και στη Γερμανία και στη Γαλλία, απηχούν, παρά τις διαφορές τους, τη συνειδητοποίηση αφενός της σημασίας της επεξεργασίας προσωπικής πληροφορίας για την άσκηση δημόσιας πολιτικής και αφετέρου των κίνδυνων που αυτή συνεπιφέρει.

Αξιοσημείωτη είναι η επιρροή της Σύμβασης 108/28.1.1981 για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα του Συμβουλίου της Ευρώπης που συνιστά την πρώτη ουσιαστική «κωδικοποίηση» των αρχών που αποτελούσαν το «σκληρό πυρήνα» της προστασίας δεδομένων προσωπικού χαρακτήρα κι αποτέλεσε την αφετηρία μιας δεύτερης «γενιάς» νομοθεσίας στην Ευρώπη [26]. Πέραν των ρυθμίσεων που αφορούσαν την ποιότητα της επεξεργασίας η Σύμβαση περιείχε ειδικούς κανόνες για τα ευαίσθητα δεδομένα καθώς και τα δικαιώματα των προσώπων, τα δεδομένα των οποίων υφίσταντο επεξεργασία. Ταυτόχρονα, έθεσε κανόνες για την προστασία των ατόμων στην περίπτωση της διασυνοριακής ροής πληροφοριών.

Σταθμός όμως για την προστασία δεδομένων προσωπικού χαρακτήρα θεωρείται η κοινοτική Οδηγία 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», με την οποία επιδιώχθηκε η εναρμόνιση των ευρωπαϊκών νομοθεσιών σε ένα υψηλό επίπεδο προστασίας [07]. Αξίζει να υπενθυμίσουμε ότι η Οδηγία εισάγει ειδικές υποχρεώσεις όσον αφορά την ασφάλεια των προσωπικών δεδομένων.

Η εισαγωγή προηγμένων ψηφιακών τεχνολογιών στα δίκτυα ηλεκτρονικών επικοινωνιών δημιούργησε ειδικές απαιτήσεις όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα και την ιδιωτική ζωή των συνδρομητών και των χρηστών. Προκειμένου να αντιμετωπιστούν τα ειδικά προβλήματα που ανακύπτουν αλλά και χάριν της ασφάλειας δικαίου και κατά συνέπεια της αποτελεσματικότερης προστασίας των

χρηστών, το κοινοτικό κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων συμπληρώθηκε από την Οδηγία 97/66/ΕΚ για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Η Οδηγία αυτή αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ για την προστασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών που τελεί και αυτή υπό τροποποίηση. Το δικαίωμα προστασίας του πολίτη από την επεξεργασία των προσωπικών του στοιχείων κατοχυρώνεται σε ορισμένα ευρωπαϊκά συντάγματα ως ένα από τα θεμελιώδη ανθρώπινα δικαιώματα.

2.2.2 Το διεθνές κανονιστικό περιβάλλον

Ως προς την αντίδραση της διεθνούς κοινότητας στους κινδύνους των ΤΠΕ για τα ανθρώπινα δικαιώματα, η απόφαση 2450/19.12.1968 της Γενικής Συνέλευσης των Ηνωμένων Εθνών κατατάσσεται στα πρώτα σχετικά κείμενα. Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) υπήρξε ο δεύτερος διεθνής οργανισμός που ασχολήθηκε με την προστασία των προσωπικών δεδομένων, εκδίδοντας τις λεγόμενες «Κατευθυντήριες Αρχές που διέπουν την προστασία της Ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων (1980). Αυτό το αρχικό και ταυτόχρονα minimum πλαίσιο γενικών αρχών στερείται δεσμευτικού χαρακτήρα και πιθανόν για το λόγο αυτό συγκέντρωσε για μεγάλο διάστημα τη συναίνεση πολλών χωρών και κυρίως εκείνων που στερούνταν (ή εξακολουθούν να στερούνται) συνολικής νομοθεσίας για την προστασία προσωπικών δεδομένων, όπως οι ΗΠΑ.

Η διαρκώς και ραγδαία αυξανόμενη διασυνοριακή ροή προσωπικών δεδομένων δημιουργεί ωστόσο συνθήκες πίεσης αναφορικά με την υιοθέτηση κανόνων και διαδικασιών που θα καθιστούν ευχερή και νόμιμη τη ροή αυτή. Μία πηγή πίεσης συνιστά η ανάγκη να εξασφαλιστεί η εμπιστοσύνη χρηστών και καταναλωτών ως προς την τύχη των δεδομένων τους. Η πίεση αυτή επιτείνεται από τη θεσμική πραγματικότητα που έχει διαμορφώσει η Ευρώπη με την Οδηγία 95/46/ΕΚ (άρθρο 25).

2.2.3 Το ελληνικό κανονιστικό πλαίσιο

Το ελληνικό νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων, όπως κατοχυρώνεται στο άρθρο 9Α του Συντάγματος, το νόμο 2472/97 (50/10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ισχύει μετά τις τροποποιήσεις που κατά καιρούς εισήχθησαν καθώς και το νόμο 3471/06 (ΦΕΚ Α' 133/28.06.2006) που αφορά την προστασία των προσωπικών δεδομένων της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Κατά την αναθεώρηση του Συντάγματος το 2001, κρίθηκε επιβεβλημένη η κατοχύρωση ενός νέου ειδικού δικαιώματος προστασίας των προσωπικών δεδομένων. Το νέο άρθρο 9Α του Συντάγματος που περιλήφθηκε στο Σύνταγμα με την τελευταία αναθεώρηση το 2001, ορίζει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, την επεξεργασία και τη χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων».

Θα μπορούσε να υποστηριχθεί, ότι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνιστά το θεμέλιο του ελληνικού συστήματος προστασίας δεδομένων επί του οποίου δομούνται το σύστημα ελέγχου και ο μηχανισμός της εφαρμογής, της τήρησης αλλά και της εξέλιξης των νομικών ρυθμίσεων. Ρήγμα στο σύστημα προστασίας επέφερε το άρθρο 8 του ν. 3625/07 που εισήγαγε την εξαίρεση ενός ευρύτατου φάσματος επεξεργασίας προσωπικών δεδομένων, συγκεκριμένα αυτής που πραγματοποιείται από τις δικαστικές-εισαγγελικές αρχές και τις διωκτικές αρχές για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων.

Ο «γενικός» νόμος συμπληρώνεται από το ν. 3471/06 για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών που αντικατέστησε τον προϊσχύοντα ν. 2774/1999 για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα. Ο νόμος αυτός, ενσωματώνοντας την Οδηγία 2002/58/ΕΚ, αποσκοπεί στην εισαγωγή ειδικών ρυθμίσεων που αφορούν το απόρρητο της επικοινωνίας και την προστασία της Ιδιωτικότητας των χρηστών από πρακτικές όπως, π.χ., η εγκατάσταση κακόβουλου λογισμικού παρακολούθησης καθώς και την οργάνωση της προστασίας των δεδομένων των συνδρομητών και των χρηστών έναντι των παροχών [35].

2.3 Η εφαρμογή των ΤΠΕ στον τομέα της προστασία της ιδιωτικής ζωής

Η εφαρμογή των τεχνολογιών της Πληροφορίας και Επικοινωνίας (ΤΠΕ) για χάρη της προστασία της ιδιωτικής ζωής έχει γίνει ευρέως γνωστή με τον όρο Τεχνολογίες Ενίσχυσης της ιδιωτικής ζωής (PET). Τα PETs έχουν οριστεί ως ένα ολοκληρωμένο σύστημα μέτρων ΤΠΕ που προστατεύουν την ιδιωτικότητα, εξαλείφοντας ή περιορίζοντας προσωπικά δεδομένα ή εμποδίζοντας την περιττή ή / και ανεπιθύμητη επεξεργασία προσωπικών δεδομένων, και όλα αυτά χωρίς να χάνεται η λειτουργικότητα των συστημάτων δεδομένων.

Τα PETs έχουν ήδη επιτύχει μια σημαντική θέση στην πρακτική και θεωρητική κατηγορία των μέσων προστασίας της ιδιωτικής ζωής, στις περισσότερες, αν όχι σε όλες τις χώρες, όπου υπάρχουν σε ισχύ νόμοι και συστήματα προστασίας δεδομένων ή που είναι σε διαδικασία δημιουργίας. Ως εκ τούτου, είναι σκόπιμο να διευκρινιστεί και να εξηγήσουμε το ρόλο των PETs που αναμένεται να παίξουν στη διαφύλαξη των προσωπικών δεδομένων και της ιδιωτικής ζωής.

Η Ευρωπαϊκή Οδηγία για την προστασία των δεδομένων 95/46 του 1995, περιλαμβάνει συνέπειες για όλους τους οργανισμούς δημόσιου και ιδιωτικού τομέα. Ο νόμος καλύπτει την επεξεργασία μηχανογραφημένων και μη ηλεκτρονικών δεδομένων, απαιτώντας τα μέρη που εμπλέκονται στην επεξεργασία των δεδομένων να διασφαλίσουν την σωστή τήρηση των κανόνων. Αυτό συνεπάγεται μια κατευθυνόμενη προσέγγιση με δραστηριότητες που πρέπει να πραγματοποιηθούν στο πλαίσιο του νόμου. Αναμένεται ότι τα προηγούμενα μέτρα και διαδικασίες όσον αφορά τον έλεγχο, την ασφάλεια και την επεξεργασία πρέπει να επανεξετασθούν και ενδεχομένως να αναθεωρηθούν.

1. Αναφορά της επεξεργασίας: Η επεξεργασία των προσωπικών δεδομένων πρέπει να αναφέρεται εκ των προτέρων στο Συμβούλιο Προστασίας Δεδομένων και στον υπεύθυνο της προστασίας της ιδιωτικής ζωής, εκτός κι αν η επεξεργασία έχει εξαιρεθεί.

2. Διαφανής επεξεργασία: Ο ενδιαφερόμενος πρέπει να είναι σε θέση να δει ποιος επεξεργάζεται τα προσωπικά του δεδομένα και για ποιο σκοπό.

3. “Όπως απαιτείται” επεξεργασία: Τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται για συγκεκριμένους, σαφείς και νόμιμους σκοπούς και δεν πρέπει να γίνεται περαιτέρω επεξεργασία με τρόπο που δεν συμβαδίζει με αυτούς τους σκοπούς.

4. Νόμιμη βάση για την επεξεργασία δεδομένων: Η επεξεργασία των προσωπικών δεδομένων πρέπει να βασίζεται σε έναν οργανισμό που αναφέρεται στο WBP, όπως η άδεια πρόσβασης, η συμφωνία, η νομική υποχρέωση, το δικαιολογημένα ενδιαφέρον και άλλα παρόμοια. Για δεδομένα όπως η υγεία, επικρατούν αυστηρότερα όρια.

5. Ποιότητα δεδομένων: Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι σωστά και όσο το δυνατόν ακριβή.

6. Δικαιώματα των συμμετεχόντων: Τα εμπλεκόμενα μέρη έχουν το δικαίωμα να λάβουν γνώση και να βελτιώσουν τα στοιχεία τους, καθώς και το δικαίωμα να προβάλουν αντιρρήσεις.

7. Κυκλοφορία δεδομένων σε χώρες εκτός της Ευρωπαϊκής Ένωσης: Κατ 'αρχήν, η κυκλοφορία των προσωπικών δεδομένων σε χώρα εκτός της ΕΕ επιτρέπεται μόνον εάν η χώρα αυτή προσφέρει επαρκή προστασία.

8. Επεξεργασία δεδομένων προσωπικού χαρακτήρα από έναν επεξεργαστή: Εάν η επεξεργασία ανατίθεται σε έναν επεξεργαστή, θα πρέπει να εξασφαλιστεί ότι τηρεί τις οδηγίες του υπευθύνου του.

9. Προστασία έναντι απώλειας και παράνομης επεξεργασίας προσωπικών δεδομένων: Κατάλληλα μέτρα τεχνικού και οργανωτικού χαρακτήρα συνθέτουν το απαραίτητο κομμάτι της νόμιμης επεξεργασίας.

2.4 Υποκλοπή ταυτότητας

Λόγω του μεγάλου όγκου των προσωπικών πληροφοριών που συχνά εμφανίζονται σε δικτυακούς τόπους κοινωνικής δικτύωσης, είναι δυνατόν να βγάλουμε παραπάνω συμπεράσματα για ένα χρήστη, οι πληροφορίες αυτές μπορεί να χρησιμοποιηθούν ως μέρος κλοπής στοιχείων ταυτότητας. Η κλοπή στοιχείων ταυτότητας πλήττει εκατομμύρια ανθρώπους ετησίως.

Κοστίζει στα θύματα ατελείωτες ώρες και χρήματα η ανάκτηση και επισκευή της ταυτότητας. Τι προκαλεί αυτό το μοντέλο ηλεκτρονικής κλοπής και απάτης; Είναι ένας συνδυασμός παραγόντων: η έλλειψη ενημέρωσης των καταναλωτών σχετικά με την προστασία της ταυτότητάς τους όταν είναι online, η άνεση και η εμπιστοσύνη στους παρόχους κοινωνικής δικτύωσης, η ανάγκη για κοινωνικές πλατφόρμες που αποφέρουν έσοδα και η έλλειψη προτύπων ή η υποχρεωτική χρήση κάποιων προτύπων. Παρά το γεγονός ότι το ζήτημα αυτό δεν είναι η κύρια προτεραιότητα, κατά πάσα πιθανότητα θα γίνει σύντομα.

2.4.1 Ο ρόλος των μέσων κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης αποκτούν έσοδα με στοχευμένη διαφήμιση, βασιζόμενοι σε προσωπικές πληροφορίες. Ως εκ τούτου, ενθαρρύνουν τους χρήστες να παρέχουν όσο το δυνατόν περισσότερες πληροφορίες για τον εαυτό τους. Με την περιορισμένη εποπτεία της κυβέρνησης, τα πρότυπα της βιομηχανίας και την έλλειψη κινήτρων να εκπαιδευτούν οι χρήστες όσον αφορά την ασφάλεια, τη προστασία της ταυτότητας και της ιδιωτικής ζωής, οι χρήστες εκτίθενται σε κλοπή ταυτότητας και απάτης.

Επιπλέον, αυτές οι πλατφόρμες έχουν εμπιστευτικές πληροφορίες των χρηστών και είναι ευάλωτες σε εξωτερικές και εσωτερικές επιθέσεις. Για λόγους μάρκετινγκ, η Google πρόσφατα κατοχύρωσε έναν αλγόριθμο για να βαθμολογεί την επιρροή του ατόμου μέσα στα κοινωνικά δίκτυα. Μόλις δημοσιοποιηθεί, θα ενθαρρύνει τη συμμετοχή των ενεργών χρηστών προκειμένου να ενισχύσουν το σκορ της επιρροή τους.

2.4.2 Εγκλήματα Ευκαιριών

Με την παγκόσμια αύξηση χρήσης των κοινωνικών δικτύων, δημιουργήθηκαν ακόμη περισσότερες ευκαιρίες για κλοπή ταυτότητας ή διάπραξη απάτης online. Για παράδειγμα, ενημερώσεις κατάστασης που δημοσιεύονται στο Twitter, Facebook και σε πολλούς άλλους τόπους κοινωνικής δικτύωσης μπορούν να χρησιμοποιηθούν από εγκληματίες. Εάν δημοσιεύσεις ότι είσαι εκτός πόλεως για διακοπές, έχεις εκτεθεί για διάρρηξη.

Αν αναφέρεις ότι είσαι εκτός πόλεως για επαγγελματικούς λόγους ένα Σαββατοκύριακο, μπορεί να αφήσεις την οικογένεια σου εκτεθειμένη σε επίθεση ή ληστεία. Όταν πρόκειται για κλοπή μιας ταυτότητας, ή χρήση φωτογραφιών και βίντεο που έχετε μοιραστεί με ιστοσελίδες όπως το Flickr και το YouTube προσφέρουν βαθύτερες γνώσεις για εσάς, την οικογένεια και τους φίλους σας, το σπίτι σας, τα αγαπημένα σας χόμπι και ενδιαφέροντα.

Σύμφωνα με τα παραπάνω, οι ιστότοποι κοινωνικής δικτύωσης έχουν τα μεγαλύτερα περιθώρια για κατάχρηση. Ενώ ο καθένας ξέρει ότι δεν πρέπει ποτέ να μοιραστεί τον αριθμό κοινωνικής ασφάλισης και την άδεια οδήγησης, πολλές ιστοσελίδες κοινωνικής δικτύωσης τα ζητάνε, εάν δεν απαιτείται, ζητούν παρόμοιες ευαίσθητες πληροφορίες που μπορούν να χρησιμοποιηθούν εναντίον σου με διάφορους κακόβουλους τρόπους.

Τα ακόλουθα στοιχεία του προφίλ μπορούν να χρησιμοποιηθούν για να κλέψουν ή να υπεξαιρέσουν την ταυτότητά σας:

• πλήρες όνομα (ιδιαίτερα το μεσαίο σου όνομα)

• ημερομηνία γέννησης (συχνά απαιτείται)

• πόλη διαμονής

• κατάσταση σχέσης

• τοποθεσία σχολείου και ημερομηνία αποφοίτησης

• ονόματα κατοικίδιων

• άλλα ενδιαφέροντα και χόμπι

2.4.3 Τύποι παραβίασης της ιδιωτικής ζωής

Πολλοί αναρωτιούνται γιατί το να μοιράζεσαι δημόσια το όνομα του κατοικίδιου ζώου σου, την ημερομηνία αποφοίτησης από το λύκειο και τη συμμετοχή σε μια οργάνωση είναι τόσο επικίνδυνη πράξη. Υπάρχουν διάφοροι λόγοι για τους οποίους πρέπει να τηρούμε το απόρρητο των προσωπικών δεδομένων, ή τουλάχιστον να τα διαχειριζόμαστε σωστά. Παρακάτω είναι μερικά μόνο παραδείγματα για το πώς κάποιες πληροφορίες μπορούν να χρησιμοποιηθούν και να θέσουν σε κίνδυνο την ταυτότητά σας:

• προσπάθειες "ψαρέματος", με τη χρήση αυτών των πληροφοριών θα προσπαθήσουν να κερδίσουν την εμπιστοσύνη σας προκειμένου να λάβουν μη δημοσιοποιημένες πληροφορίες μέσω online συνομιλιών. Η εταιρεία Portland Oregon USA, πρόσφατα επιτέθηκε με ψευδείς καταγγελίες στην Better Business Bureau, προκειμένου να λάβει επιπλέον πληροφορίες σχετικά με την εταιρεία και τους εργαζομένους της.

• η ενεργοποίηση του GPS στα τηλέφωνα, μέσω αυτής της διαδικασίας δημοσιεύετε στο κοινό η τοποθεσία που βρίσκεστε και μπορεί να αποκαλυφθούν ευαίσθητες πληροφορίες, όπως η διεύθυνση του σπιτιού σας, η διεύθυνση εργασίας και τα μέρη που επισκέπτεστε.

• 95% των προφίλ στο Facebook έχουν τουλάχιστον μία εφαρμογή, πολλές από τις οποίες δεν αξιολογούνται και μπορεί να χρησιμοποιηθούν για κακόβουλους και εγκληματικούς σκοπούς.

• ψεύτικο προφίλ, μπορεί να χρησιμοποιηθεί για απάτη ή να δυσφημήσει ένα χαρακτήρα. Ένας Καναδός ρεπόρτερ πρόσφατα δυσφημίστηκε μέσω ψεύτικου προφίλ που περιλάμβανε παραπλανητικές δημοσιεύσεις, όσον αφορά τις ομάδες που είναι μέλος και για τις πολιτικές του θέσεις.

• Αμερικανός στρατιώτης στο Ιράκ, ανακάλυψε τον τραπεζικό του λογαριασμό επανειλημμένα να έχει παραβιαστεί διαδικτυακά και να του τραβάνε χρήματα. Ένας ειδικός σε θέματα ασφαλείας ήταν σε θέση να αποκτήσει πρόσβαση στο λογαριασμό του απλά παίρνοντας στοιχεία από το όνομά του, το e-mail και το προφίλ του στο Facebook.

2.4.4 Οι ιστότοποι κοινωνικής δικτύωσης διευκολύνουν το ηλεκτρονικό έγκλημα

Ένα άλλο μειονέκτημα των δικτυακών τόπων κοινωνικής δικτύωσης είναι ότι επιτρέπουν σε άλλους να γνωρίζουν προσωπικές πληροφορίες ενός ατόμου, τα ενδιαφέροντα, τις συνήθειες, και τα μέρη που επισκέπτεται. Οι συνέπειες της χρήσης αυτών των πληροφοριών μπορεί να είναι από ακίνδυνες ως και ενοχλητικές, όπως η αύξηση των spam ως και σε κάτι πολύ επικίνδυνο, όπως η καταδίωξη.

Ενώ η συντριπτική πλειοψηφία των ανθρώπων που χρησιμοποιούν τις ιστοσελίδες κοινωνικής δικτύωσης δεν αποτελούν απειλή, υπάρχουν κακόβουλα άτομα τα οποία λόγω τις μεγάλης προσβασιμότητας και της ποσότητας προσωπικών πληροφοριών που διατίθενται σε αυτούς, μπορούν να τα χρησιμοποιήσουν εναντίον κάποιων χρηστών.

Υπάρχουν εγκληματίες που μπορούν να χρησιμοποιήσουν πληροφορίες που παρέχονται, σχετικά με τα γενέθλια ενός ατόμου, την τοποθεσία, τη ρουτίνα του, τα χόμπι και τα ενδιαφέροντά του, και να υποδυθεί έναν φίλο που θα κερδίσει την εμπιστοσύνη του εύκολα ή να πείσει το ανυποψίαστο αυτό άτομο να του δώσει πρόσβαση σε προσωπικά ή οικονομικά δεδομένα. Μπορούν να χρησιμοποιήσουν τέτοιες πληροφορίες για να μαντέψουν κωδικούς πρόσβασης λογαριασμού, γι' αυτό το λόγο δεν πρέπει ποτέ να χρησιμοποιείτε ως κωδικό πρόσβασης όνομα κατοικίδιου ζώου, όνομα αγαπημένου συγκροτήματος, χόμπι, γενέθλια, ή κάτι άλλο που προκύπτει εύκολα γνωρίζοντας κάποιες πληροφορίες για το άτομό σας. Οι διώκτες εκτιμούν ιδιαίτερα όταν δημοσιεύεται online η καθημερινή ρουτίνα και η τοποθεσία που βρίσκονται οι χρήστες!

Πρέπει λοιπόν, να προσέχετε όταν αποφασίζετε να δημοσιεύσετε κάτι, διότι όσο περισσότερες πληροφορίες έχουν τα κακόβουλα άτομα για τον οποιονδήποτε, τόσο πιο εύκολο είναι γι' αυτούς να επωφεληθούν.

2.4.5 Οι κίνδυνοι για παιδιά και τους εφήβους

Τα παιδιά και οι νέοι έφηβοι είναι ιδιαίτερα ευπαθείς στις απειλές που οι ιστοσελίδες κοινωνικής δικτύωσης παρουσιάζουν. Παρά το γεγονός ότι πολλές από αυτές τις ιστοσελίδες έχουν περιορισμούς ηλικίας, δεν υπάρχει τρόπος για να επιβάλλονται αυτές τις απαιτήσεις και τα παιδιά μπορούν να παραποιούν τις ηλικίες τους, έτσι ώστε να μπορούν να ενταχθούν.

Εγκληματίες μπορεί να στοχεύουν σε παιδιά, εφήβους, και άλλα ανυποψίαστα άτομα που βρίσκονται online. Μερικές φορές παρουσιάζονται ως κάποιοι άλλοι και στη συνέχεια, σιγά-σιγά τους προσεγγίζουν δημιουργώντας σχέσεις μαζί τους και τελικά τους πείθουν να συναντηθούν από κοντά.

Οι γονείς θα πρέπει να διδάσκουν τα παιδιά τους σχετικά με την ασφάλεια στο Διαδίκτυο, να είναι ενήμεροι για τις διαδικτυακές συνήθειες των παιδιών τους, και να χρησιμοποιούν όλα τα εργαλεία και τους πόρους που έχουν στη διάθεσή τους. Να καθοδηγούν τα παιδιά σε κατάλληλες ιστοσελίδες και να καταρτίζουν τους έφηβους ώστε να αναγνωρίζουν το ακατάλληλο περιεχόμενο και τις επαφές που δεν έχουν ζητήσει. Η λήψη αυτών των μέτρων θα βοηθήσει τα παιδιά και τους εφήβους να γίνουν υπεύθυνοι και ασφαλείς χρήστες υπολογιστών.

2.5 Βέλτιστες Πρακτικές Προστασίας

Προτού να μεταβείτε σε ακυρώσεις όλων των λογαριασμών κοινωνικής δικτύωσης, σκεφτείτε ότι υπάρχουν τρόποι όπως το να προσέχετε τι θα μοιράζεστε και με ποιους τα μοιράζεστε. Ακολουθώντας τις βέλτιστες πρακτικές που περιγράφονται παρακάτω, μπορείτε να απολαύσετε τα οφέλη των μέσων κοινωνικής δικτύωσης, χωρίς να κάνετε τον εαυτό σας στόχο για τους εγκληματίες.

Ρυθμίσεις απορρήτου

Βεβαιωθείτε ότι γνωρίζετε ποιες πληροφορίες μοιράζονται δημόσια και ποιες πληροφορίες μπορούν να χρησιμοποιηθούν από τις εφαρμογές. Μπορεί να μοιράζεστε περισσότερες πληροφορίες απ' ότι έχετε σκοπό. Να θυμάστε να φροντίζετε να προσαρμόζετε τις ρυθμίσεις της ιδιωτικής σας ζωή, διότι όταν επισκέπτεστε τις ιστοσελίδες άλλων, μπορεί αυτοί να είναι σε θέση να λαμβάνουν πληροφορίες από το λογαριασμό σας στο Facebook, συμπεριλαμβάνοντας το όνομά σας, τη φωτογραφία του προφίλ και τα ενδιαφέροντά σας. Για περισσότερες πληροφορίες σχετικά με τις ρυθμίσεις του Facebook, επισκεφθείτε το πολιτική χρήσης δεδομένων.

Ισχυροί κωδικοί πρόσβασης

Δημιουργείστε πολύπλοκους κωδικούς πρόσβασης με τουλάχιστον 10 χαρακτήρες, με ανάμειξη γραμμάτων, συμβόλων και αριθμών (μη χρησιμοποιείτε λέξεις που μπορούν να βρεθούν σε ένα λεξικό). Θα πρέπει επίσης να αποφεύγετε την επαναχρησιμοποίηση των ίδιων κωδικών πρόσβασης στις διάφορες ιστοσελίδες διότι εάν ο κωδικός πρόσβασης έχει παραβιαστεί, οι εγκληματίες του κυβερνοχώρου θα έχουν στη συνέχεια πρόσβαση σε όλους τους λογαριασμούς σας. Εάν χρησιμοποιείτε ένα δημόσιο υπολογιστή, βεβαιωθείτε ότι δεν κρατάει τη διεύθυνση του ηλεκτρονικού σας ταχυδρομείου και τον κωδικό πρόσβασής σας. Είναι εύκολο να επιλέξετε κατά λάθος «να με θυμάσαι», γι' αυτό μην ξεχνάτε να κοιτάτε πέρα από τις ρυθμίσεις απορρήτου του περιηγητή σας.

Προσοχή στην επιλογή «φίλων»

Είναι ένας καλός εμπειρικός κανόνας να συνδέεστε και να μοιράζεστε μόνο με ανθρώπους που γνωρίζετε στην πραγματική ζωή. Αν κάνετε "φίλους" ανθρώπους που είναι ξένοι, εκτίθεστε και υπάρχει κίνδυνος ασφάλειας και προστασίας της ιδιωτικής σας ζωής. Σύμφωνα με μια μελέτη από το Cloudmark, σχεδόν το 40% των νέων προφίλ στο Facebook είναι ψεύτικα και δημιουργήθηκαν από κακόβουλα προγράμματα και spammers.

Προσεκτική επιλογή υλικού προς δημοσίευση

Προσωπικές πληροφορίες, όπως ημερομηνία γέννησης, διεύθυνση κατοικίας, διεύθυνση ηλεκτρονικού ταχυδρομείου μπορούν να χρησιμοποιηθούν για μια ποικιλία από απάτες, ακόμη και για κλοπή ταυτότητας. Σκεφτείτε πόσο πολύτιμη πληροφορία θα ήταν για κάποιους να κρατήσουν ημερομηνίες και λεπτομέρειες από ταξίδια, τις διακοπές σας και το χρόνο που δαπανάτε μακριά από το σπίτι σας.

Προσοχή στους ύποπτους συνδέσμους

Πολλές απάτες και κακόβουλα λογισμικά στον κόσμο των κοινωνικών δικτύων έχουν εξαπλωθεί μέσω συνδέσμων και εφαρμογών απατεώνων. Μπορεί να έχετε δει πρόσφατες δημοσιεύσεις όπως "Φοιτητής επιτέθηκε στον καθηγητή του και σχεδόν τον σκότωσε" με ένα σύνδεσμο να επισυνάπτεται στη δημοσίευση αυτή. Προσέχετε όταν κάνετε κλικ σε συνδέσμους ακόμα και αν προέρχονται από φίλους. Πολλές από αυτές τις εφαρμογές μόλις τις εγκαθιστάς δίνουν πρόσβαση στα στοιχεία σας που δημοσιεύονται, χωρίς να το γνωρίζετε.

Περιορισμός στη χρήση εφαρμογών

Εφαρμογές λογισμικού που είναι διαθέσιμες με download για να τρέξουν στην ιστοσελίδα σας, δεν μπορεί να έχουν υποβληθεί σε οποιοδήποτε είδος ελέγχου ασφαλείας, επαλήθευσης ή κριτικής. Οι εφαρμογές αυτές μπορούν να χρησιμοποιηθούν από τους απατεώνες του κυβερνοχώρου και να θέσουν σε κίνδυνο τις πληροφορίες σας. Μπορεί να δημοσιεύσετε προσωπικές σας πληροφορίες στο προφίλ σας αλλά και στους προγραμματιστές των εφαρμογών, όταν εγκαταστήσετε τη νέα εφαρμογή, ακόμα και αν χρησιμοποιείτε ρυθμίσεις απορρήτου.

Παρακολουθήστε τα παιδιά σας

Οι ιστοσελίδες κοινωνικής δικτύωσης μπορεί ενδεχομένως να οδηγήσουν τα παιδιά, τους νεαρούς αλλά και τους ενήλικες σε πολύ αρνητικές πτυχές του Διαδικτύου, συμπεριλαμβανομένης της παρενόχλησης, σε online αρπακτικά και απάτες στον κυβερνοχώρο. Σιγουρευτείτε ότι έχετε προετοιμάσει τα παιδιά σας και τους έχετε δώσει πληροφορίες που τους βοηθούν να παίρνουν σωστές αποφάσεις και να ενημερώνονται για την ασφαλή και ορθή χρήση του διαδικτύου.

Άμεση αντίδραση σε ύποπτες ενέργειες

Υπάρχουν διάφοροι τρόποι για να αναφέρεις πιθανά spam ή απάτες. Αν νομίζετε ότι ο λογαριασμός σας έχει παραβιαστεί, αλλάξτε αμέσως τον κωδικό πρόσβασής σας. Εάν εμφανίζονται στο Facebook ενημερώσεις κατάστασης που δεν έχετε κάνει, αυτό σημαίνει ότι μπορεί να έχετε εγκαταστήσει μια εφαρμογή απάτης. Αφαιρέστε την ύποπτη εφαρμογή από το προφίλ σας στο Facebook, καθώς και το σχετικό μήνυμα από την κατάστασή σας. Τα νέα σας, αυτά που σας αρέσουν και τα ενδιαφέροντα σας επεξεργαστείτε τα από το μενού "Επεξεργασία του προφίλ μου".

Συνεχής ενημέρωση για πρόσφατες απάτες

Αυτό είναι πιο εύκολο στα λόγια παρά στην πράξη, αλλά λίγη προσοχή και ευαισθητοποίηση μπορεί να βοηθήσει να μην εμπίπτουμε σε online τεχνάσματα, τα οποία γίνονται ολοένα και πιο στοχευμένα. Στο Lavasoft, υπάρχει μια σειρά από πόρους που διατίθενται, προκειμένου να καταστήσουν τη διαδικασία ταχύτερη και ευκολότερη: διαβάστε συμβουλές για ασφάλεια στο Lavasoft Security Center, ελέγξτε το blog της εταιρείας Lavasoft και Malware Labs blog για την ασφάλεια των καθημερινών ειδήσεων, και ακολουθήστε το Lavasoft στο Facebook ή το Twitter για να μείνετε ενημερωμένοι για θέματα ασφαλείας.

Βασικό λογισμικό ασφαλείας

Προστατέψτε τον υπολογιστή σας με Anti-Virus, Anti-Spyware και Firewall (να διασφαλίσετε ότι το λογισμικό ενημερώνεται συχνά) είναι κρίσιμης σημασίας να προστατεύεστε από κακόβουλα λογισμικά και ηλεκτρονικές απάτες. Για αξιόπιστες λύσεις ασφαλείας, ελέγξτε την ιστοσελίδα Lavasoft στο www.lavasoft.com .

Ειδικά στους ιστότοπους κοινωνικής δικτύωσης

Πρέπει να βάζετε όρια όσον αφορά ποιος μπορεί να δει ό,τι δημοσιεύετε. Αν δεν θέλετε οποιοσδήποτε χρήστης να δει τα στοιχεία επικοινωνίας σας, μπορείτε να περιορίσετε τη δημοσίευση των εν λόγω δεδομένων. Απλά αλλάξτε τις ρυθμίσεις σας. Μπορείτε επίσης να αποκλείσετε κάποιους χρήστες να έχουν οποιαδήποτε επαφή μαζί σας.

Μια απλή και γρήγορη ρύθμιση (στο Facebook) για να αυξήσετε την προστασία της ιδιωτικής σας ζωής, είναι να περιορίσετε την προβολή του προφίλ σας μόνο σε χρήστες που είναι στις λίστες των φίλων σας. Οι περισσότεροι ιστότοποι κοινωνικής δικτύωσης προσφέρουν παρόμοιους τρόπους για να περιοριστεί η πρόσβαση σε προσωπικές πληροφορίες, αλλά σε όλες τις περιπτώσεις η αρχή είναι η ίδια: μη διαφημίζετε στον κόσμο τι κάνετε ή που ζείτε.

Αλλά μην ξεχνάτε ότι ακόμα και αν περιορίζετε ποιος μπορεί να δει τι δημοσιεύετε, υπάρχουν τρόποι όπου μπορεί κάποιος να δει το προφίλ σας έτσι κι αλλιώς. Συνεπώς περιορίστε τις δημοσιεύσεις σας. Μην μοιράζεστε πράγματα που θα σας κάνουν ευάλωτους σε κακόβουλους χρήστες (όπως να μοιράζεστε τη διεύθυνση του ηλεκτρονικού σας ταχυδρομείου, φυσική διεύθυνση, ή τον αριθμό τηλεφώνου) ή σε έμμονη παρακολούθηση (όπως πληροφορίες για το πρόγραμμα ή την ρουτίνα σας).

Επίσης, αν οι φίλοι σας δημοσιεύουν πληροφορίες σχετικά με εσάς, βεβαιωθείτε ότι η συνδυασμένη πληροφορία που διατίθενται από τις σελίδες τους δεν είναι αρκετή να σας κάνουν να νιώθετε άβολα που ξένοι θα έχουν αυτές τις πληροφορίες για εσάς.

2.6 SNS - social network services

Στο σημείο αυτό πρέπει να κάνουμε μία σύντομη αναφορά στα σύγχρονα μέσα κοινωνικής δικτύωσης. Μια υπηρεσία κοινωνικής δικτύωσης, συχνά καλείται SNS- social network service, είναι το μέσο στο οποίο άτομα μοιράζονται ίδια ενδιαφέροντα ή / και δραστηριότητες.

Οι ιστοσελίδες κοινωνικής δικτύωσης επιτρέπουν στους χρήστες να μοιράζονται ιδέες, δραστηριότητες, εκδηλώσεις, και τα ενδιαφέροντά τους εντός των δικτύων αυτών. Οι περισσότερες υπηρεσίες των κοινωνικών δικτύων είναι web-based και παρέχουν τα μέσα στους χρήστες για να αλληλεπιδρούν με διάφορους τρόπους, όπως e-mail και άμεσων μηνυμάτων.

Τα σύγχρονα κινητικά τηλέφωνα με συνεχή σύνδεση στο διαδίκτυο, συμμετέχουν πολύ στη σύνδεση με τα SNS και την ενσωμάτωση με τις διάφορες υπηρεσίες και τα κάνει ακόμη πιο δημοφιλή. Υπάρχουν πάρα πολλά δίκτυα κοινωνικής δικτύωσης, αλλά στην παρούσα εργασία θα αναφερθούμε στα παρακάτω τρία πιο δημοφιλή από αυτά.

2.6.1 Facebook

Η αρχική ιστοσελίδα του facebook ήταν αρχικά περιορισμένη και τη χρησιμοποιούσαν μόνο οι φοιτητές του Harvard, αλλά πολύ γρήγορα επεκτάθηκε και σε άλλα κολέγια στην περιοχή της Βοστώνης, σε άλλα Ivy League σχολεία, και τελικά επεκτάθηκε σε κάθε πανεπιστήμιο της Βόρειας Αμερικής, μέχρι σήμερα, όπου ένας στους επτά ανθρώπους της γης είναι γραμμένος στο Facebook. Ιδρύθηκε από τον Mark Zuckerberg μαζί με κάποιους από τους συγκατοίκους και συμφοιτητές του στο Πανεπιστήμιο του Χάρβαρντ, συμπεριλαμβανομένων τον Eduardo Saverin, τον Dustin Moskovitz, τον Andrew McCollum και τον Chris Hughes.

Το Facebook ωστόσο, θεωρητικά ξεκίνησε στις 23 Οκτώβρη του 2003, όταν ο Zuckerberg ξεκίνησε το Facemash.com. Το Facemash έδινε τη δυνατότητα στους επισκέπτες (κυρίως τους φοιτητές του Χάρβαρντ) να συγκρίνουν δύο φωτογραφίες φοιτητών και να λένε ποιος ήταν "καυτός" και ποιος "όχι".

thefacebook.com

Στις 11 Ιανουαρίου του 2004 ο Zuckerberg ανέβασε στο διαδίκτυο το thefacebook.com. Σε ένα άρθρο στην εφημερίδα "The Harvard Crimson" αναφέρθηκε ότι ο Zuckerberg εμπνεύστηκε από το Facemash και δημιούργησε το Facebook, "Είναι σαφές ότι η τεχνολογία που απαιτείται για να δημιουργηθεί μια δημόσια ιστοσελίδα είναι άμεσα διαθέσιμη ... και τα οφέλη είναι πολλά". Ο Mark επίσης δήλωσε ότι ήθελε να δημιουργήσει μια ιστοσελίδα που να μπορούν όλοι να συνδέονται με το Πανεπιστήμιο. Σκέφτηκε ότι το Χάρβαρντ θα χρειαστεί πολλά χρόνια για να εφαρμόσει ένα τέτοιο σύστημα, κάτι που ο ίδιος μαζί με τους φίλους του θα μπορούσαν να το θέσουν σε λειτουργία σε μια εβδομάδα. Σημεία σταθμοί:

Σεπτέμβριος 2006: το Facebook αρχίζει να αφήνει οποιονδήποτε πάνω από 13 ετών να συμμετέχει. Επίσης, εισάγει το News Feed, το οποίο συλλέγει δημοσιεύσεις φίλων από τους τοίχους τους σε ένα συγκεκριμένο μέρος. Παρόλο που οδήγησαν σε καταγγελίες για την προστασία της ιδιωτικής ζωής, το News Feed έγινε το πιο δημοφιλή χαρακτηριστικό του Facebook.

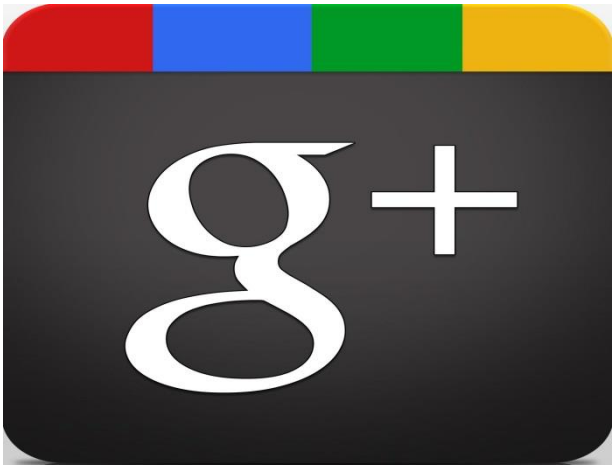
Ιούνιος 2009: το Facebook ξεπερνά το Myspace Corp' s News και θεωρείται το κορυφαίο online κοινωνικό δίκτυο στις ΗΠΑ.

Αύγουστος 2010: το Facebook εγκαινιάζει τη λειτουργία των εγκαταστάσεών του, επιτρέποντας σε φίλους και ξένους να τους επισκεφθούν.

Ιανουαρίου 2013: το Facebook ανακοινώνει την έναρξη του Graph Search, που επιτρέπει στους χρήστες να αναζητούν οτιδήποτε οι φίλοι τους έχουν μοιραστεί, συμπεριλαμβανομένων φωτογραφιών και μηνυμάτων.

2.6.2 Google+

Για να κατανοήσουμε την εξέλιξη του νέου εγχειρήματος της Google, ας ρίξουμε μια ματιά στη πρόσφατη ιστορία του διαδικτύου. Από το 2009, οι χρήστες του Facebook έχουν τη δυνατότητα να δηλώνουν ότι τους "αρέσει" [25] το περιεχόμενο που αναρτάται από τους φίλους τους, μια κίνηση που επιτρέπει στους χρήστες να έχουν πρόσβαση σε άλλους, χωρίς να γράψουν κάποιο σχόλιο. Αυτή η απλή αλλαγή, ελαχιστοποίησε τα εμπόδια για είσοδο και συμμετοχή και αύξησε τη κοινωνική αλληλεπίδραση σε ολόκληρη την πλατφόρμα. Στο συνέδριο των προγραμματιστών F8, τον Απρίλιο του 2010, το Facebook ανακοίνωσε ότι το κουμπί "Like" δεν θα είναι πλέον διαθέσιμο για ιστοσελίδες τρίτων να το εγκαταστήσουν (50.000 ιστοσελίδες αντέδρασαν μέσα στη πρώτη εβδομάδα μετά την ανακοίνωση).



Όσες ιστοσελίδες τρίτων χρησιμοποιούσαν το κουμπί "Like" είχαν σημαντικές συνέπειες. Ενώ παλαιότερα ένα "Like" ήταν μια καθαρά κοινωνική ενέργεια, ως απάντηση σε μια δημοσίευση ενός φίλου, το νέο "Like" αναμειγνύει τις εμπορικές και κοινωνικές πτυχές του Διαδικτύου. Το νέο "Like" έγινε εργαλείο για να επισημάνεις το ενδιαφέρον σου για το περιεχόμενο μιας σελίδας, όπως θα έκανε κάποιος και σ' ένα blog , αλλά και ως επίδειξη υποστήριξης μιας μεγάλης φίρμας, όπως θα μπορούσε κάποιος να κάνει "Like" στη Nike.

Οι Φίρμες αντιλήφθηκαν γρήγορα την αξία του "Like", ως ένα είδος δωρεάν διαφήμισης και ως μέτρο για δημοσιότητα. Οι φίρμες συμφωνούν ότι το "Like" είναι καλό να υπάρχει.

Το πραγματικό χτύπημα όμως, ήταν η ανακοίνωση της ενσωμάτωσης μεταξύ των "Likes" του Facebook και των αποτελεσμάτων αναζήτησης της Microsoft Bing. Στο πλαίσιο των ανακοινώσεων του "Open Graph", το Facebook και η Microsoft αποκάλυψαν ότι οι αναζητήσεις θα περιλαμβάνουν τα "Like" από τους φίλους στο Facebook κάτω από τα αποτελέσματά τους. Αυτό όχι μόνο κάνει τις αναζητήσεις περισσότερο σχετικές με το χρήστη, αλλά έχει επίσης μια επιπλέον επίπτωση για τις επιχειρήσεις: οι άνθρωποι αναφέρουν ότι εμπιστεύονται πιο πολύ τις απόψεις των φίλων τους από τις διαφημίσεις. Το κουμπί "Like" σήμερα λειτουργεί ως σφραγίδα έγκρισης από φίλους.

Ουσιαστικά, στο Google+ έχετε την ευκαιρία να αυξήσετε το SEO (search engine optimization) σας, ενθαρρύνοντας τους χρήστες να "+1" τη σελίδας σας. Οι αλγόριθμοι αναζήτησης της Google έχουν αρχίσει να λαμβάνουν υπόψη πόσα "+1s" έχετε, χρησιμοποιώντας το ως δείκτη ποιότητας και σπουδαιότητας. Αυτό είναι καλό νέο διότι παρέχουν αξία στις νόμιμες ιστοσελίδες, δεδομένου ότι κανείς δεν πρόκειται να πατήσει "+1" σε μια ιστοσελίδα που έχει φορτωμένα φτωχού λεξιλογίου άρθρα. Αν και δεν γνωρίζουμε ακόμη πώς ακριβώς το "+1" θα χρησιμοποιηθεί μέσα από τους αλγόριθμους της Google, είναι ασφαλές να πούμε ότι οι συνειδητοποιημένοι

διαχειριστές θα αρχίσουν να ενσωματώνουν το Google Plus στη SEO (search engine optimization) στρατηγική τους.

Η Google εδώ και καιρό έχει βάλει σαν στόχο να φτάσει τους 500 εκατομμύρια χρήστες του Facebook, και θεώρησε την ενσωμάτωση του Facebook με το Bing ως απειλή. Είχαν μια αποτυχημένη προσπάθεια να δημιουργήσουν ένα κοινωνικό δίκτυο το Google Buzz, και αναγκάστηκαν να ξανασχεδιάσουν και να δημιουργήσουν το Google+.

2.6.3 Twitter

Το Twitter είναι ένα micro-blogging δίκτυο δημοσιεύσεων πραγματικού χρόνου, με περιορισμό 140 χαρακτήρων ή λιγότερο.

Το Twitter ξεκίνησε ως ιδέα από τον Jack Dorsey το 2006. Ο Dorsey είχε αρχικά φανταστεί το Twitter ως μια SMS-based πλατφόρμα επικοινωνίας. Ομάδες φίλων μπορούσαν να ενημερώνονται για το τι κάνουν άλλοι, βασισμένοι στις ενημερώσεις της κατάστασής τους.

Κατά τη διάρκεια μια συνεδρίας καταιγισμού ιδεών στο podcasting της εταιρείας Odeo, ο Jack Dorsey πρότεινε τη δημιουργία αυτής της SMS-based πλατφόρμας επικοινωνίας στον συνιδρυτή της Odeo, Evan Williams. Ο Evan, είναι και συνιδρυτής του Biz Stone, κατ 'επέκταση, έδωσε στον Jack το πράσινο φως να ξοδέψει περισσότερο χρόνο για το έργο αυτό και να το αναπτύξει περαιτέρω.

Όριο 140 χαρακτήρων

Ο λόγος που υπάρχει τέτοιος περιορισμός, είναι γιατί το Twitter είχε αρχικά σχεδιαστεί ως μια πλατφόρμα βασισμένη σε SMS μηνύματα κινητών τηλεφώνων. Οι 140 χαρακτήρες, ήταν το όριο μηνυμάτων των συσκευών κινητής τηλεφωνίας σύμφωνα με τα πρότυπο των SMS πρωτοκόλλων. Το Twitter, τελικά εξελίχθηκε σε μια διαδικτυακή πλατφόρμα και το όριο των 140 χαρακτήρων παρέμεινε. Σκεφτείτε το ως ένα δημιουργικό περιορισμό.

Αρχικά οι χρήστες του Twitter δεν είχαν τη δυνατότητα να απαντήσουν ή να φωνάξουν ο ένας τον άλλον. Ορισμένοι χρήστες όμως περιλαμβάνουν ένα σύμβολο @ πριν από το όνομα χρήστη για να αναγνωρίζουν κάποιον άλλο χρήστη μέσα σε ένα Tweet. Αυτό έγινε με τόσο διαδεδομένο τρόπο, δηλαδή να αναγνωρίζει έναν άλλο χρήστη, που η ομάδα του Twitter πρόσθεσε τη λειτουργία αυτή στην πλατφόρμα του Twitter. Το ίδιο πράγμα συνέβη με τα hashtags, τα οποία αποτελούν πλέον αναπόσπαστο μέρος του οικοσυστήματος του Twitter.

Σεπτέμβριος 2011: το Twitter φτάνει τους 100 εκατομμύρια ενεργούς χρήστες, οι οποίοι στέλνουν περίπου ένα δισεκατομμύριο tweets κάθε πέντε ημέρες και 230 εκατομμύρια tweets κάθε ημέρα.

Σε έξι χρόνια, οι χρήστες του Twitter έχουν αυξηθεί σε πάνω από 200 εκατομμύρια ενεργούς χρήστες το μήνα. Το Μάρτιο του 2013, οι Jack Dorsey και Biz Stone βραβεύτηκαν με δίπλωμα ευρεσιτεχνίας γι' αυτό που εφάρμοσαν το 2007, και αφορά όλο το σύστημα του Twitter.

Κεφάλαιο 3

PETs- Privacy Enhancing Technologies

Στο κεφάλαιο αυτό θα αναφερθούμε στα πιο σημαντικά είδη τεχνολογιών προστασίας της Ιδιωτικότητας. Πρέπει να σημειωθεί ότι οι τεχνολογίες αυτές βρίσκονται σε βασικό επίπεδο. Προστατεύουν όχι μόνο στο κομμάτι της χρήσης των δικτύων κοινωνικής δικτύωσης αλλά και στην πλοήγηση στο διαδίκτυο, αλλά και στην ανταλλαγή αρχείων. Στην προστασία της Ιδιωτικότητας, από τα ίδια τα δίκτυα κοινωνικής δικτύωσης θα αναφερθούμε σε επόμενο κεφάλαιο.

Η χρήση των PETs συμβάλλει στην ανάπτυξη συστημάτων και υπηρεσιών, πληροφόρησης και επικοινωνίας κατά τρόπο που ελαχιστοποιεί τη συλλογή και τη χρήση των προσωπικών δεδομένων και διευκολύνει τη συμμόρφωση με τους κανόνες προστασίας των δεδομένων. Η χρήση των PETs θα συμβάλει ώστε η παραβίαση ορισμένων κανόνων προστασίας δεδομένων να καταστεί δυσχερέστερη και να μπορεί να ανιχνευθεί.

Αρκετά παραδείγματα PETs μπορούν να αναφερθούν εδώ και μία εξαιρετικά ενημερωμένη λίστα παρουσιάζεται παρακάτω [36].

- Αυτόματη ανωνυμοποίηση μετά από ένα ορισμένο χρονικό διάστημα, υποστηρίζουν την αρχή ότι η επεξεργασία των δεδομένων, θα πρέπει να διατηρείται σε μορφή που να επιτρέπει τον προσδιορισμό των υποκειμένων των δεδομένων για διάστημα όχι μεγαλύτερο από όσο είναι αναγκαίο, για τους σκοπούς για τους οποίους έχουν συλλεχθεί.

- Εργαλεία κρυπτογράφησης, που εμποδίζουν το hacking όταν η πληροφορία μεταδίδεται μέσω του Διαδικτύου και υποστηρίζει την υποχρέωση του υπεύθυνου επεξεργασίας δεδομένων να λαμβάνει τα κατάλληλα μέτρα για την προστασία των προσωπικών δεδομένων από αθέμιτη επεξεργασία.

- Cookie-κόπτες, που αποκλείουν τα cookies να τοποθετούνται στον υπολογιστή του χρήστη και να διενεργούν ορισμένες ενέργειες χωρίς αυτός να είναι ενήμερος. Εντείνουν τη συμμόρφωση με την αρχή, ότι τα δεδομένα πρέπει να υφίστανται θεμιτή και νόμιμη επεξεργασία και ότι ο ενδιαφερόμενος των δεδομένων πρέπει να ενημερώνεται για την εξέλιξη της επεξεργασίας.

- Πλατφόρμα για προτιμήσεις απορρήτου (P3P), που επιτρέπει στους χρήστες του Διαδικτύου, να αναλύουν τις πολιτικές απορρήτου των ιστοσελίδων και να τις συγκρίνουν με τις προτιμήσεις του χρήστη ως προς τις πληροφορίες που επιτρέπει να απελευθερώσει, βοηθά να εξασφαλιστεί η συγκατάθεση του ενδιαφερόμενου των δεδομένων για την επεξεργασία των δεδομένων έχοντας απόλυτη επίγνωση.

Στρατηγικές PET: Αναγνώριση και το Κριτήριο της Δυσανάλογης προσπάθειας

Κατά την εφαρμογή των PETs, ο ενδιαφερόμενος μπορεί να επιλέξει δύο στρατηγικές: Είτε εστιάζοντας σε πρόληψη ή τη μείωση της αναγνώρισης, είτε δίνοντας έμφαση στην πρόληψη της παράνομης επεξεργασίας των προσωπικών δεδομένων. Ένας συνδυασμός και των δύο είναι μία επίσης πιθανή επιλογή.

Όσον αφορά την πρώτη επιλογή, τα PETs περιλαμβάνουν συνέπειες για τα προσωπικά δεδομένα στο πλαίσιο των συστημάτων δεδομένων. Για να προσδιοριστεί αυτό, πρέπει να είναι σαφές ποια είναι δεδομένα προσωπικού χαρακτήρα. Από άποψη νομικής, προσωπικά δεδομένα νοείται κάθε πληροφορία σχετικά με ένα συγκεκριμένο φυσικό πρόσωπο.

Σύμφωνα με το άρθρο 2 της οδηγίας 95/46, ένα φυσικό πρόσωπο μπορεί να αναγνωριστεί "άμεσα ή έμμεσα". Άμεση ταυτοποίηση απαιτεί βασικά στοιχεία (π.χ. όνομα, διεύθυνση, κ.λπ.), καθώς και ένα προσωπικό αριθμό, γνωστός ως ψευδο-ταυτότητα, ένα βιομετρικό χαρακτηριστικό όπως ένα δακτυλικό αποτύπωμα, κλπ. Η έμμεση αναγνώριση απαιτεί άλλα μοναδικά χαρακτηριστικά ή ιδιότητες ή ένα συνδυασμό των δύο, για να παρέχουν επαρκή πληροφορία αναγνωρίσεως.

Τα PETs το καθιστούν δυνατό, να καταστήσουν ανώνυμα ή να "μη ταυτοποιούνται" άμεσα τα στοιχεία ταυτότητας. Όταν τα δεδομένα δεν μπορούν να προσδιοριστούν από τα χαρακτηριστικά τους, τότε μπορεί να μιλήσει κανείς για μια κατάσταση στην οποία δεν υπάρχουν προσωπικά δεδομένα και οι προστατευτικές διατάξεις του οδηγού δεν ισχύουν πλέον.

Η μη-ταυτοποίηση μπορεί επίσης να συμβεί, εάν η ποσότητα και η φύση των στοιχείων έμμεσου προσδιορισμού είναι τέτοια ώστε η ταυτοποίηση του ατόμου είναι δυνατή μόνο με την εφαρμογή των δυσανάλογων προσπαθειών, ή με τη βοήθεια τρίτου προσώπου εκτός αρχής και εξουσίας είναι απαραίτητη. Το να μιλήσουμε για δυσανάλογη προσπάθεια εξαρτάται, αφενός, από τη φύση των δεδομένων και το μέγεθος του πληθυσμού, και από την άλλη πλευρά, από τους πόρους χρόνου και χρήματος που κάποιος είναι πρόθυμος να ξοδέψει προκειμένου να είναι σε θέση να προσδιορίσει το πρόσωπο.

Στρατηγικές PET: Ασφάλεια κατά περιττής Επεξεργασίας

Τα PETs μπορούν επίσης να εφαρμοστούν για προστασία ενάντια σε διάφορες μορφές παράνομης επεξεργασίας προσωπικών δεδομένων, όπου συμπεριλαμβάνεται η παράνομη συλλογή, καταγραφή, αποθήκευση, αποκάλυψη (εντός ή μεταξύ οργανισμών), αντιστοίχιση ή κοινή χρήση.

Κατά την εφαρμογή των PETs σε αυτές τις πτυχές επεξεργασίας, ο ενδιαφερόμενος μπορεί να επιλέξει να διαμορφώσει τα δεδομένα του σε ένα σύστημα που χρησιμοποιεί για πεδία την ταυτότητα και την ψευδο-ταυτότητα, έτσι ώστε λίγα ή καθόλου προσωπικά δεδομένα να μπορούν να μπουν σε διαδικασία επεξεργασίας (για παράδειγμα, κατά τη συλλογή ή την εγγραφή) και να εξαρτώνται από τα πρωτόκολλα του συστήματος δεδομένων, για την παροχή ή πρόσβαση σε ανώνυμα στοιχεία, που επιτρέπεται ή δεν επιτρέπεται στους διάφορους χρήστες.

Για παράδειγμα, για επιστημονική έρευνα και στατιστική επεξεργασία, μπορεί να χορηγηθεί πρόσβαση σε μη αναγνωρίσιμα δεδομένα, ενώ για τα νοσοκομεία, αναγνωρισμένα δεδομένα μπορούν να παρέχονται κάτι το οποίο βασίζεται στην άδεια λειτουργίας του νοσοκομείου και της σχέση μεταξύ του παρόχου περίθαλψης και του ασθενή.

Επιπλέον, όταν εξετάζουμε την επεξεργασία των δεδομένων έναντι των πολιτικών προστασίας με θεμιτή και νόμιμη επεξεργασία, τα PETs μπορούν να εκπληρώσουν ένα σημαντικό ρόλο, αυτός είναι, εάν η δοκιμή δείχνει ότι ορισμένα στοιχεία δεν μπορούν να υποβληθούν σε επεξεργασία ή ότι μόνο τα απολύτως απαραίτητα στοιχεία μπορούν να δεχθούν επεξεργασία. Αν ο "όπως απαιτείται" χαρακτήρας έχει καθοριστεί και τα PETs εφαρμοστούν στο πλαίσιο του δίκαιου και του νόμιμου, μπορούν να συμβάλουν στη διατήρηση του "όπως απαιτείται" όρων συμφωνίας.

Με το χρόνο και την πείρα παρατηρείται ότι τα PETs προσφέρουν πλεονεκτήματα απόδοσης στη πολιτική επεξεργασίας δεδομένων, για παράδειγμα με την απλούστευση των διαδικασιών, την αποφυγή της γραφειοκρατίας μέσω better_business διεργασίες, ή την ενίσχυση της ασφάλειας. Ωστόσο, η εφαρμογή των PETs σε παλιά συστήματα δεδομένων δεν είναι πάντοτε εφικτή. Για παράδειγμα, το άνοιγμα υφιστάμενων συστημάτων δεδομένων για να εισάγουν έναν προστάτη ταυτότητας μπορεί να είναι πολύ ακριβό. Επιπλέον, ο ιδιοκτήτης του παλαιού

συστήματος δεδομένων συχνά δεν διαθέτει το θάρρος και τη θέληση να διεξάγει τέτοιες λειτουργίες.

Οι μεγάλες ευκαιρίες για τα PETs είναι, στο σχεδιασμό και την εφαρμογή των νέων συστημάτων δεδομένων. Τα τελευταία συστήματα δεδομένων συχνά δεν συμμορφώνονται πλήρως με τις απαιτήσεις που καθορίζονται από το Νόμο περί Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή της σχετικής νομοθεσίας. Για να εφαρμοστούν αποτελεσματικά οι απαιτήσεις που διατυπώθηκαν στη νομοθεσία, είναι σημαντικό να συνειδητοποιήσουμε ότι πρέπει να έχουμε ένα κατάλληλο σύστημα, με γενικά μέτρα επεξεργασίας και διαδικασίες που βασίζονται στη προστασία των διεργασιών της εταιρείας και σε συνδυασμό με ειδικά μέτρα προστασίας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Έχει ήδη αναφερθεί ότι τα PETs, είναι ένα εξαιρετικό μέσο για να εφαρμοστεί αποτελεσματικά και να ενισχύσει μια ισορροπημένη πολιτική για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Οργανωτικά μέτρα θα εξακολουθήσουν να απαιτούνται, εκτός από τα προληπτικά τεχνικά μέτρα που προβλέπονται από τα PETs, στο κομμάτι της αξιοπιστίας υπάρχουν πολλοί λόγοι για τους οποίους προτιμούνται τα PETs.

Πώς μπορεί η ποιότητα των PETs να εγγυηθεί για συγκεκριμένες εφαρμογές;

Οι κοινωνίες δείχνουν μια αυξανόμενη ζήτηση για άμεση και αδιαμφισβήτητη κατανόηση της ποιότητας των προϊόντων και των υπηρεσιών, και τα PETs ενδέχεται να πρέπει να αποδείξουν την αξία τους. Τέτοιες δηλώσεις ποιότητας συχνά εκφράζονται μέσω μιας πιστοποίησης που εκδίδεται από έναν εμπειρογνώμονα ή ανεξάρτητο τρίτο πρόσωπο.

Η εν λόγω πιστοποίηση μπορεί να διαδραματίσει σημαντικό ρόλο στη διευκρίνιση αν τα PETs μπορούν να εφαρμοστούν αποτελεσματικά σε ένα σύστημα δεδομένων. Για την έκδοση αυτής της πιστοποίησης, τα PETs ακολουθούν μια συγκεκριμένη διαδικασία πιστοποίησης. Οι πιστοποιήσεις δείχνουν ότι το εν λόγω σύστημα δεδομένων έχει κατασκευαστεί με τέτοιο τρόπο ώστε να μπορεί να αναφέρεται με βεβαιότητα ότι με τη βοήθεια των PETs, η επιδιωκόμενη προστασία των προσωπικών δεδομένων έχει όντως παρασχεθεί.

Η τεχνική αυτή εμφανίζει ομοιότητα με τις εκτιμήσεις των επιπτώσεων της ιδιωτικής ζωής, οι οποίες τυγχάνουν τη προσοχή σε πολλές χώρες, ως μέρος της προστασίας των δεδομένων. Οι ερευνητές της επιστήμης των υπολογιστών προσπαθούν να μετρήσουν το επίπεδο παροχής προστασίας της Ιδιωτικότητας, υπολογιστικά, της θεωρίας της πληροφορίας και την τέλεια ανωνυμία, μελετώντας τα διάφορα συστήματα.

Ίσως σε πέντε χρόνια, με τη χρήση ενός "μέτρου προστασίας της ταυτότητας" θα δίνετε feedback στους χρήστες σχετικά με το επίπεδο προστασίας. Για παράδειγμα να δείχνουν ότι το επίπεδο της ανωνυμίας είναι χαμηλό σε δίκτυα υψηλής κυκλοφορίας, με την προειδοποίηση ότι ο κίνδυνος που έχει παρατηρηθεί για διαρροή προσωπικών δεδομένων είναι υψηλό. Αυτό σημαίνει ότι η εισαγωγή των PETs σε συστήματα δεν είναι μόνο μια τεχνική εργασία, αλλά και εργασία κανονιστική και αξιολογική.

Συμπερασματικά

Οι εξελίξεις στον τομέα των ΤΠΕ προσφέρουν ακόμα περισσότερες δυνατότητες για συλλογή, αποθήκευση, επεξεργασία προσωπικών δεδομένων. Οι πιθανές παραβιάσεις της Ιδιωτικότητας των καταναλωτών και των πολιτών της κατά συνέπεια αυξάνεται.

Ωστόσο, οι ίδιες οι ΤΠΕ προσφέρουν λύσεις για τη προστασία της Ιδιωτικότητας των χρηστών, των καταναλωτών και των πολιτών. Τα PETs είναι μια πολλά υποσχόμενη βοήθεια για την επίτευξη βασικών στόχων προστασίας της ιδιωτικής ζωής με νόμιμη επεξεργασία των δεδομένων. Φυσικά, η προσοχή και η έρευνα για τα PETs είναι απαραίτητη, και οι αρχές προστασίας δεδομένων θα πρέπει να συνεχίσουν να καταβάλλουν κάθε δυνατή προσπάθεια για την ενίσχυση εφαρμογών PET στα συστήματα δεδομένων.

Πολλές χώρες προτρέπουν τους πολίτες να χρησιμοποιούν PETs, θεωρείται μέρος μιας ολοκληρωμένης και συστηματικής προσέγγισης για την προστασία της ιδιωτικής ζωής και αποδίδει σημαντικό ρόλο στα τεχνολογικά μέσα προστασίας, χωρίς την παραδοχή ότι είναι μια "μαγική σφαίρα", ότι μπορούν να απευθύνονται στο στόχο χωρίς νομικά, οργανωτικά, ηθικά και εκπαιδευτικά εργαλεία.

Θα πρέπει επίσης να ελεγχθεί, αν τα PET όντως συμμορφώνονται με τη νομοθεσία προστασίας της ιδιωτικής ζωής. Πιστοποίηση που εμπίπτει στον έλεγχο της ιδιωτικής ζωής μπορεί να συμβάλει σε αυτό και να προσφέρουν την αναγκαία ασφάλεια στον πολίτη και καταναλωτή, ότι ισχύει το απόρρητο των προσωπικών του δεδομένων και προστατεύονται αποτελεσματικά. Στο σημείο αυτό θα αναφερθούμε στους κυριότερους και πιο διαδεδομένους τύπους PET.

3.1 Ad-blockers (αποκλεισμός διαφημίσεων)

Οι Ad-blockers είναι φίλτρα περιεχομένου, που βασίζονται σε προκαθορισμένες λίστες φίλτρων για να εντοπίζουν και να εξαλείφουν διαφημίσεις. Λειτουργούν μεταγλωττίζοντας λίστες εκφράσεων που σχετίζονται με τις διαφημίσεις και χρησιμοποιούν πρότυπα αντιστοίχισης, τα οποία συγκρίνουν με τα εξερχόμενα αιτήματα που προκύπτουν από το πρόγραμμα περιήγησης του χρήστη.

Ο αποκλεισμός διαφημίσεων μπορεί επίσης να εμποδίσει script παρακολούθησης, τα οποία με τη σειρά τους εμποδίζουν δίκτυα διαφημίσεων τρίτων από την προβολή διαφημίσεων στο πρόγραμμα περιήγησης ενός χρήστη μέσω της ιστοσελίδας του εκδότη. "Πριν εμφανιστεί η σελίδα, ο Adblock Plus την τροποποιεί, σειρές αιτήσεων για την υπηρεσία διαφημίσεων ή script παρακολούθησης και διοχετεύει ένα CSS για την επισκευή της ιστοσελίδας ώστε να μην φαίνεται χαλασμένη" λέει η Till Faida, πρόεδρος του Adblock Plus.

Σκεφτείτε το σαν χειρουργική αφαίρεση των διαφημίσεων και στη συνέχεια κλείνουμε τις τρύπες. Για τον χρήστη δεν υπάρχει καμία απόδειξη ότι υπήρξε ποτέ διαφήμιση. Διακόπτουν τις επικοινωνίες με δίκτυα διαφημίσεων τρίτων, ειδικοί αναστολείς παρακολούθησης όπως η Disconnect επίσης αποκλείει διαφημίσεις από τέτοιου είδους πηγές. Η Disconnect λειτουργεί εξετάζοντας το όνομα του κεντρικού υπολογιστή για κάθε εξερχόμενη αίτηση του προγράμματος περιήγησης και αποκλείει αιτήσεις προς κεντρικούς υπολογιστές που συνδέονται με δίκτυα διαφημίσεων, που παρακολουθούν τη δραστηριότητα των χρηστών σε ολόκληρη την ιστοσελίδα. Αλλά η πρόθεση είναι να εμποδίσουν την παρακολούθηση, όχι τις διαφημίσεις, λέει ο συν-διευθύνων σύμβουλος Casey Oppenheim[13], και τα εργαλεία αυτά εξακολουθούν να αφήνουν να περάσουν διαφημίσεις που παράγονται από τον εκδότη.

Οι χρήστες ιστοσελίδων τυχερών παιχνιδιών και τεχνολογίας είναι πιο πιθανό να αποκλείσουν διαφημίσεις, απ' ότι οι αναγνώστες οικονομικών και ταξιδιωτικών ιστοσελίδων, πιθανότατα επειδή οι τεχνολογικά ενημερωμένοι αναγνώστες γνωρίζουν ότι υπάρχουν αναστολείς διαφημίσεων και πώς να τις εγκαταστήσουν. Άτομα που χρησιμοποιούν το Firefox της Mozilla και το Chrome της Google είναι πιο πιθανό να μπλοκάρουν τις διαφημίσεις, ίσως επειδή πολλά εργαλεία κλειδώματος διαφημίσεων για πρώτη φορά διατέθηκαν σε αυτά τα προγράμματα περιήγησης.

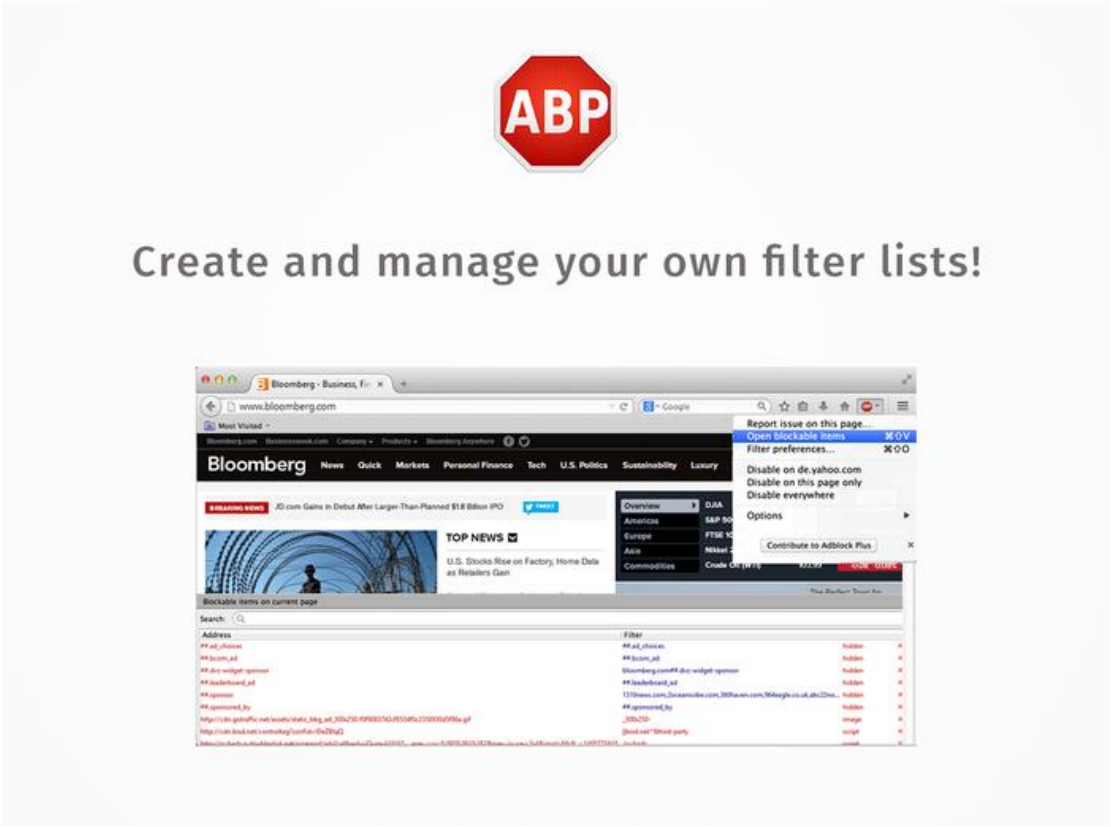
Αυτό δείχνει, ότι οι καταναλωτές βρίσκουν δικούς τους τρόπους για να αποφύγουν ενοχλητικές για την ιδιωτική τους ζωή επεμβατικές διαφημίσεις, αντί να περιμένουν κυβερνητική παρέμβαση για την online παρακολούθηση και στοχευμένη διαφήμιση.

Όμως, η επιθυμία για την προστασία της ιδιωτικής ζωής μας οδηγεί σε μια πιο γρήγορη, πιο καθαρή εμπειρία περιήγησης και το κόστος το χρεώνονται οι εκδότες. Ο αριθμός των ατόμων που δέχεται διαφημίσεις μικραίνει συνεχώς, με αποτέλεσμα οι διαφημίσεις να γίνονται πιο επιθετικές και παρεμβατικές προς τους στόχους τους, με αποτέλεσμα αυτά τα άτομα να εκνευρίζονται και να αναζητούν αναστολείς διαφημίσεων. Όλο αυτό είναι ένας φαύλος κύκλος. Ακολουθεί μία λίστα με τους πιο δημοφιλείς αναστολείς διαφημίσεων.

3.1.1 AdBlock Plus (ABP)

Το AdBlock Plus (ABP) είναι ένα από τα πιο δημοφιλή Ad-blockers, με εκδόσεις για τον Firefox, Chrome, Opera, και μια νέα έκδοση που μόλις κυκλοφόρησε για τον Internet Explorer. Το ABP διαθέτει γρήγορη εγκατάσταση, φορτώνει προκαθορισμένες λίστες φίλτρων που επιτρέπουν στους χρήστες να μπλοκάρουν γρήγορα τις περισσότερες διαφημίσεις, καθώς και τη δυνατότητα να φιλτράρουν για κακόβουλο λογισμικό στα μέσα κοινωνικής δικτύωσης.

Συνειδητοποιημένοι χρήστες μπορούν να επιλέξουν και να προσθέσουν επιπλέον block λίστες, όπως και να βάλουν προσαρμοσμένα φίλτρα ή λίστες επιτρεπόμενων. Το Adblock Plus προσφέρει αυτό που λέμε "μη ενοχλητικές διαφημίσεις" μέσα από φίλτρα, το οποίο μπορεί να ενοχλεί κάποιους χρήστες, αλλά μπορεί να απενεργοποιηθεί στις ρυθμίσεις.



3.1.2 AdBlock (Chrome, Opera, Safari)

Το AdBlock (καμία σχέση με το AdBlock Plus) είναι ένας άλλος αναστολέας διαφημίσεων, διαθέσιμος για τους χρήστες του Chrome, Opera και Safari. Ο AdBlock χρησιμοποιεί μια σειρά από λίστες φίλτρων για να μπλοκάρει αυτόματα το περιεχόμενο των διαφημίσεων που προέρχονται από γνωστούς διακομιστές διαφημίσεων και παρόχων.

Οι χρήστες μπορούν να χρησιμοποιούν μόνο τις λίστες αποκλεισμού της προεπιλογής, αλλά μπορούν να γραφτούν και σε άλλες λίστες, ή ακόμη να δημιουργήσουν δικές τους λίστες, καθώς να φτιάξουν και λίστες αποκλειόμενων ιστοσελίδων ή περιεχομένου. Το AdBlock έχει την εμπιστοσύνη πολλών χρηστών σε όλο τον κόσμο.

3.1.3 NoScript (Firefox)

Το NoScript εμποδίζει τα Java, JavaScript και άλλα plugins που μπορούν να χρησιμοποιηθούν ως διαφημίσεις ή δείκτες κακόβουλων προγραμμάτων επίθεσης. Εμφανίζεται ως ένα μικρό κουμπί στην κάτω δεξιά γωνία του παραθύρου του Firefox. Το NoScript μπορεί να ρυθμιστεί για να μπλοκάρει scripts σε παγκόσμιο επίπεδο, επιλεκτικά, ή να αφήνει συγκεκριμένες ιστοσελίδες να υπάρχουν σε μια μόνιμη ή προσωρινή βάση, καθώς και λίστες αποκλειόμενων ιστοσελίδων και παρόχων.

Η υψηλή δυνατότητα προσαρμογής και οι κορυφαίες δυνατότητες που προσφέρει, κάνουν το NoScript ένα μεγάλο εργαλείο για την ασφάλεια και αναστολή των διαφημίσεων, είτε από μόνο του, είτε σε συνδυασμό με άλλους αναστολείς διαφημίσεων. Σημειώστε ότι το NoScript μπορεί να χαλάσει κάποια λειτουργία ενός διαδικτυακού τόπου.

3.1.4 ScriptSafe (Chrome)

Το ScriptSafe είναι ένα εργαλείο του Chrome εμπνευσμένο από το NoScript, προκειμένου να παράσχει μια παρόμοια λειτουργικότητα αποκλεισμού script στους χρήστες του Chrome. Δυστυχώς, λόγω τεχνικών λεπτομερειών στο σχεδιασμό του Chrome, το ScriptSafe αλλά και άλλα παρόμοια προγράμματα δεν μπορούν να φτάσουν τη λειτουργικότητα του NoScript για το Firefox. Πρέπει να σημειώσουμε, ότι τα άτομα που εργάστηκαν για το ScriptSafe έκαναν μια πολύ καλή προσπάθεια, επιτρέποντας στους χρήστες να μπλοκάρουν σε διαφορετικά επίπεδα, δημιουργώντας μαύρες λίστες ή λίστες επιτρεπόμενων πεδίων, και πολλά άλλα.

3.1.5 Flashblock (Firefox, Chrome)

Μια άλλη δημοφιλής επέκταση με λειτουργικότητα αναστολής διαφημίσεων είναι το Flashblock (Firefox, Chrome), μια επέκταση φιλτραρίσματος περιεχομένου που εμποδίζει Flash, Silverlight,

HTML5 βίντεο, και παρόμοιο περιεχόμενο να παιχτούν. Το Flashblock αφήνει στοιχεία κράτησης θέσης στα οποία οι χρήστες επιλεκτικά μπορούν να κάνουν κλικ πάνω τους, για να παίξουν και να δούνε συγκεκριμένα στοιχεία ή βίντεο. Καθώς πολλές από τις πιο ενοχλητικές διαφημίσεις χρησιμοποιούν βίντεο, μουσική ή ηχητικά εφέ βασίζονται σε Flash και παρόμοια εργαλεία, το Flashblock μπορεί να μειώσει την ενόχληση είτε μόνο του είτε με άλλες επεκτάσεις.

3.2 Anonymous Web Surfing

Το Anonymous Web Surfing , επιτρέπει σε κάθε χρήστη να επισκεφθεί τοποθεσίες Web, χωρίς να επιτρέπει σε οποιονδήποτε να συγκεντρώσει πληροφορίες σχετικά με το ποιες ιστοσελίδες επισκέπτεται ο χρήστης. Οι υπηρεσίες που παρέχουν ανωνυμία, απενεργοποιούν τα αναδυόμενα παράθυρα, τα cookies και αποκρύπτουν την IP διεύθυνση του επισκέπτη. Οι υπηρεσίες αυτές συνήθως χρησιμοποιούν ένα διακομιστή μεσολάβησης για την επεξεργασία κάθε HTTP αίτησης. Όταν ο χρήστης αιτείται για μια ιστοσελίδα κάνοντας κλικ σε μια υπερ-σύνδεση ή πληκτρολογώντας μια διεύθυνση URL στο πρόγραμμα περιήγησής του, η υπηρεσία ανακτά και εμφανίζει τις πληροφορίες χρησιμοποιώντας το δικό του server.

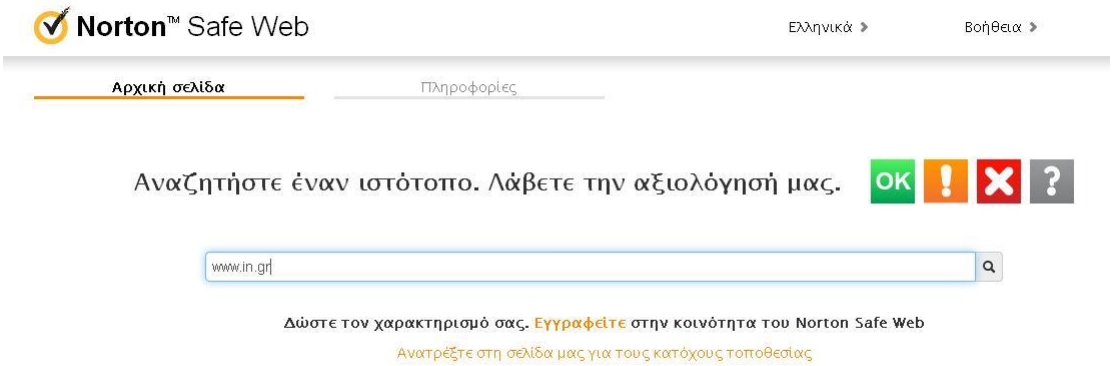
Ο απομακρυσμένος διακομιστής (όπου βρίσκεται η ιστοσελίδα που ζητήθηκε) λαμβάνει πληροφορίες σχετικά με τον Anonymous Web Surfing αντί για πληροφορίες του χρήστη. Το Anonymous Web Surfing είναι δημοφιλής για δύο λόγους: για την προστασία της ιδιωτικής ζωής του χρήστη και παρακάμπτει τον αποκλεισμό εφαρμογών που θα εμποδίσουν την πρόσβαση του σε δικτυακούς τόπους ή σε συγκεκριμένα μέρη των ιστοσελίδων που ο χρήστης θέλει να επισκεφθεί.

Μία ανώνυμη υπηρεσία περιήγησης μπορεί να κάνει ένα χρήστη να αισθάνεται πιο ασφαλής στο Διαδίκτυο, αλλά δεν επιτρέπει μια ιστοσελίδα να προσωποποιεί τον επισκέπτη. Αυτό σημαίνει ότι μία ιστοσελίδα, δεν μπορεί να προσαρμόσει το περιεχόμενο ή τις διαφημίσεις να ταιριάζουν με κάθε χρήστη. Το Norton Safe Web και το Anonymizer είναι η πιο συχνά χρησιμοποιούμενες υπηρεσίες.

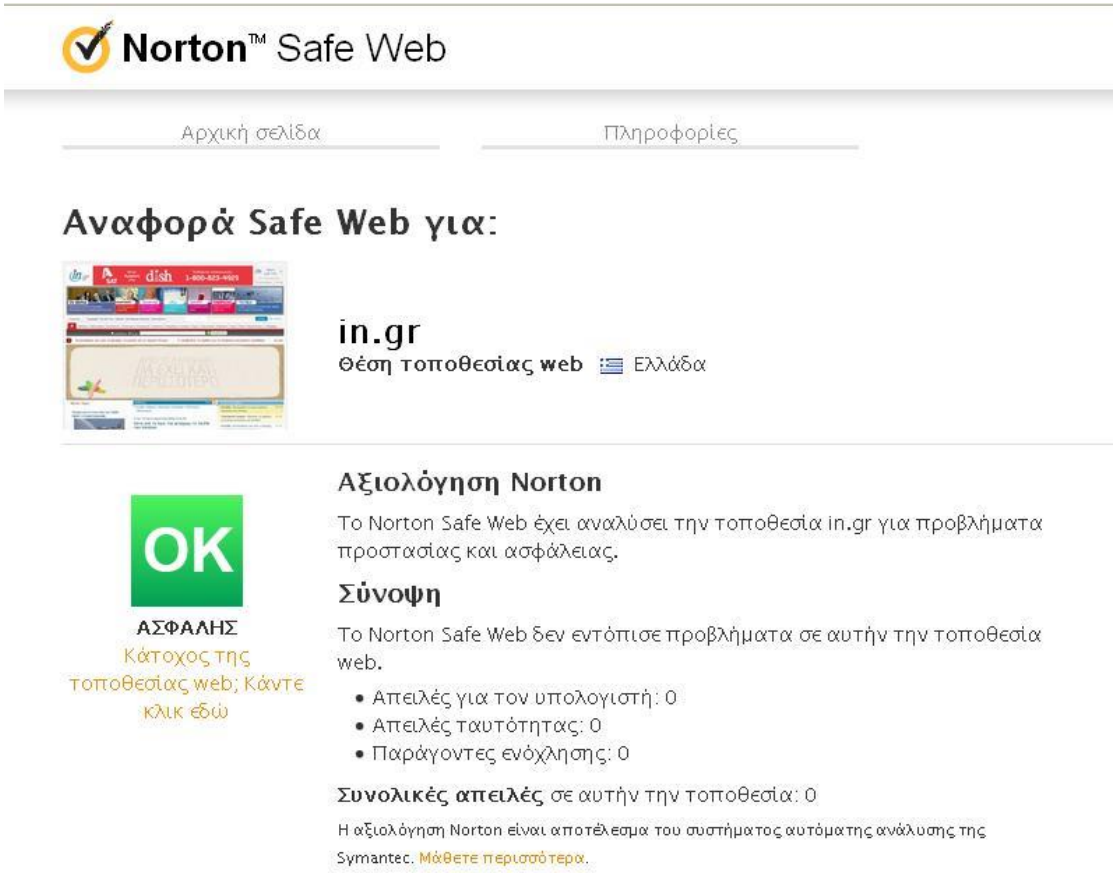
3.2.1 Norton Safe Web

Το Norton Safe Web είναι μια νέα υπηρεσία αξιοπιστίας από τη Symantec . Οι διακομιστές της εταιρείας αναλύουν τοποθεσίες στο web ώστε να εξακριβώσουν πώς θα επηρεάσουν τους χρήστες και τον υπολογιστή τους. Έπειτα ενημερώνουν για την ασφάλεια κάποιας συγκεκριμένης τοποθεσίας του web πριν από την προβολή της, μέσω της γραμμής εργαλείων του Norton που έχει εγκατασταθεί στον υπολογιστή.

Στην παρακάτω εικόνα φαίνεται ο τρόπος με τον οποίο λειτουργεί το Norton Safe Web. Εισάγουμε στο πεδίο αναζήτησης την δικτυακή τοποθεσία, της οποίας την αξιολόγηση ως προς την ασφάλεια θέλουμε να ελέγξουμε.



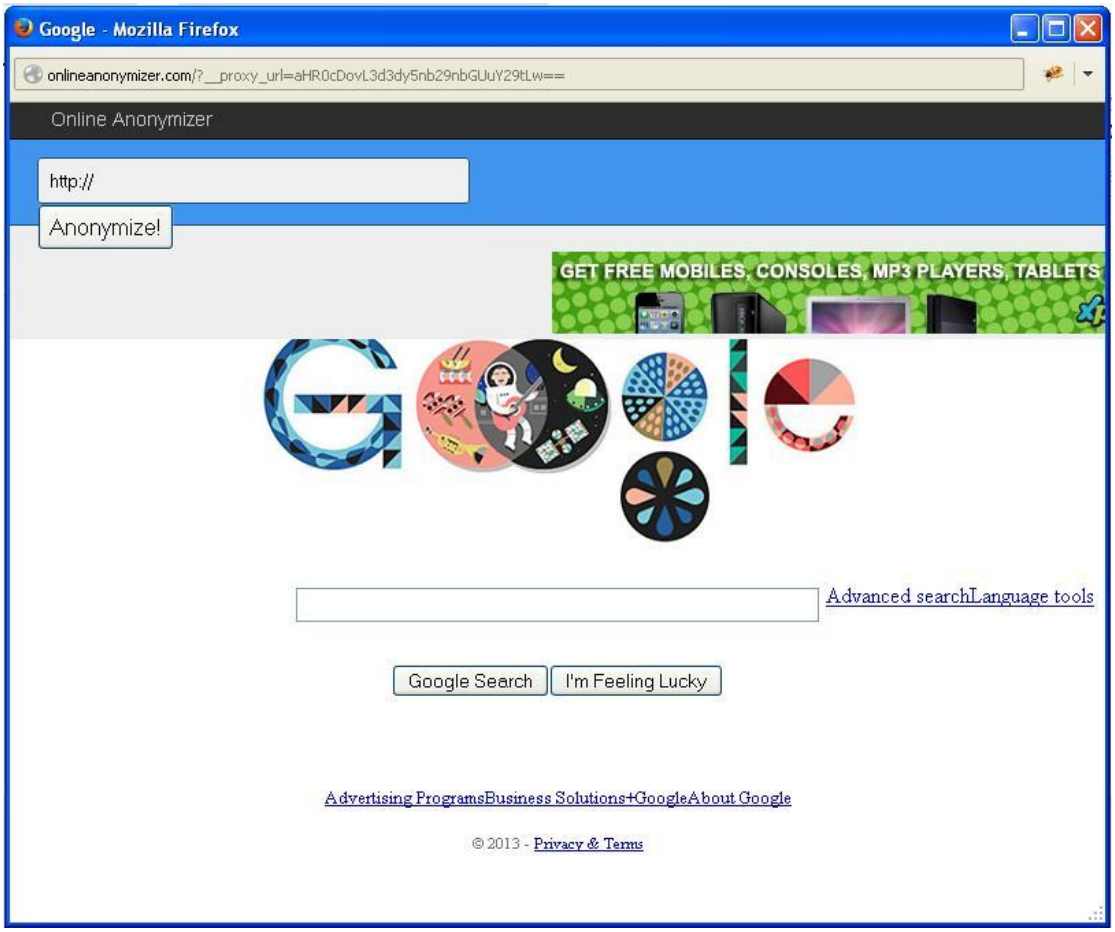
Το Norton Safe Web χρησιμοποιεί δικό του αλγόριθμο για να προσδιορίσει διάφορους τύπους απειλών και επιστρέφει μία αναφορά.



3.2.2 Online Anonymizer

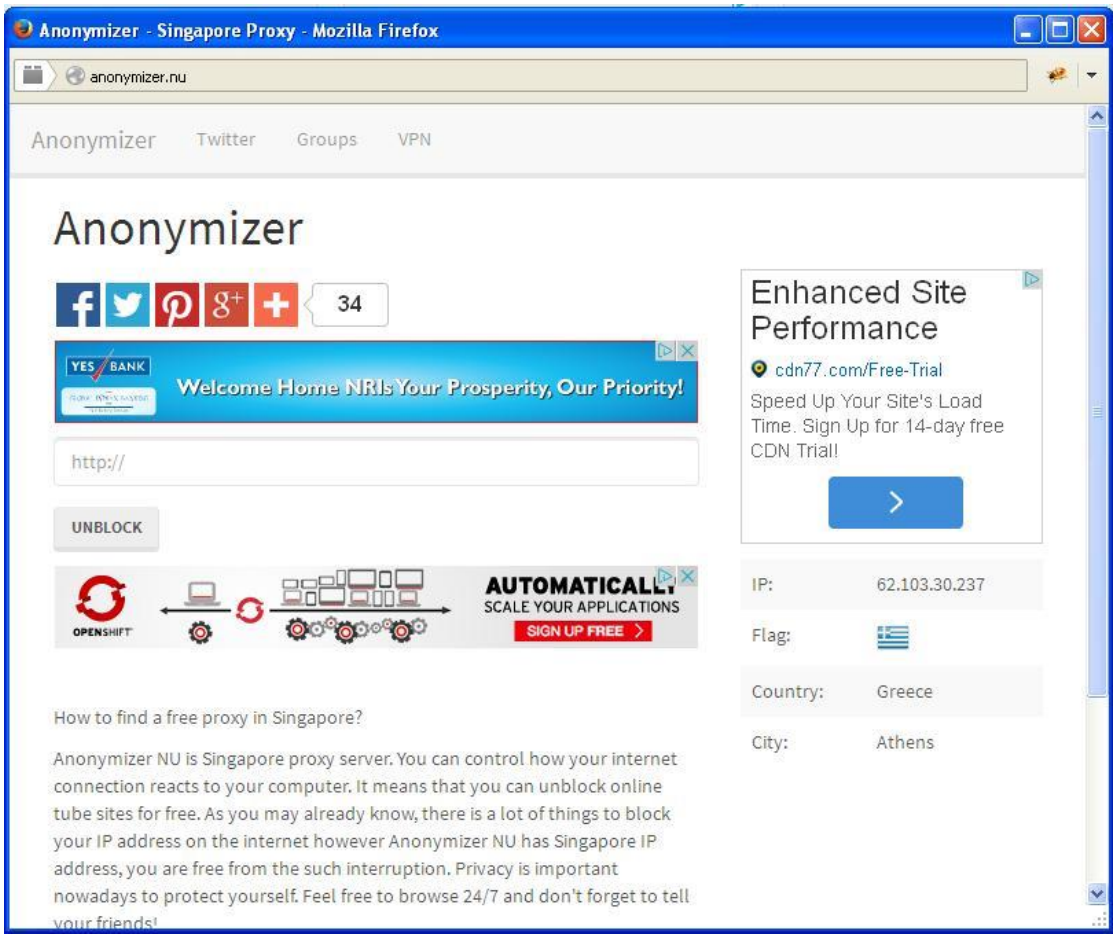
Το Online Anonymizer στοχεύει στην παροχή ενός γρήγορου και ασφαλή τρόπου για να την απεμπλοκή ιστοσελίδων και να περιηγηθείτε σε παλιά φίλτρα του web τα οποία μπορεί να λογοκρίνουν την περιήγησή σας. Ο δωρεάν Anonymous διακομιστής παρακάμπτει όλα αυτά τα web blog που εμποδίζουν την ελευθερία στο Διαδίκτυο.

Η διεύθυνση IP του Anonymizer σας επιτρέπει επίσης να κρύψετε την IP σας όταν είστε online, και σας δίνει ανώνυμες δυνατότητες περιήγησης. Μπορείτε να κινείστε με μυστικότητά στο web χρησιμοποιώντας το Online Anonymizer για τις ανάγκες της περιήγησής σας.



3.2.3 Anonymizer NU- Singapore Proxy

Το Anonymizer NU είναι ένας διακομιστής μεσολάβησης της Σιγκαπούρης. Μπορεί να ελέγξει, πως η σύνδεσή σου στο Internet αντιδρά με τον υπολογιστή σου. Αυτό σημαίνει ότι μπορείς να καταργήσεις τον αποκλεισμό των δωρεάν online ιστοσελίδων. Όπως γνωρίζουμε υπάρχουν πολλά που μπορούν να αποκλείσουν την IP διεύθυνση μας στο διαδίκτυο, ωστόσο το Anonymizer NU έχει IP διεύθυνση Σιγκαπούρης, οπότε δεν υπάρχει περίπτωση για τέτοια διακοπή.



3.2.4 Stealth Anonymizer

Το Stealth Anonymizer λειτουργεί σε συνδυασμό με διακομιστές μεσολάβησης για να παρέχουν τη πιο δυνατή ιδιωτική πλατφόρμα, ώστε να μπορείτε να περιηγηθείτε στο διαδίκτυο. Όλες οι δραστηριότητες σας στο διαδίκτυο, συμπεριλαμβανομένων και της περιήγησης σε ιστοσελίδες, η χρήση του Gmail ή άλλες υπηρεσίες ηλεκτρονικής αλληλογραφίας, η κοινή χρήση αρχείων και άλλες λήψεις, γίνονται εντελώς ανώνυμα. Η βάση δεδομένων των ανώνυμων διακομιστών μεσολάβησης ενημερώνεται συνεχώς, οπότε υπάρχει πάντα καλή σύνδεση.

Το Stealth Anonymizer αποκλείει επίσης και τα cookies, διαγράφει το ιστορικό περιήγησης και εμφανίζει την τρέχουσα ταχύτητα της σύνδεσής σας στο Internet. Μπορείτε να κρατήσετε τον υπολογιστή ή το φορητό υπολογιστή προστατευμένο και ασφαλή, καθώς μπορείτε επίσης να προστατεύσετε ολόκληρο το ασύρματο ή τοπικό δίκτυο σας.

3.3 VPN – virtual private network

Το VPN είναι ένα δίκτυο που κατασκευάζεται με τη χρήση δημόσιων καλωδίων - συνήθως το διαδίκτυο - για να συνδεθείτε σε ένα ιδιωτικό δίκτυο, όπως το εσωτερικό δίκτυο μιας εταιρείας. Υπάρχουν μια σειρά από συστήματα που σας επιτρέπουν να δημιουργήσετε δίκτυα που χρησιμοποιούν το Διαδίκτυο ως μέσο για τη μεταφορά δεδομένων. Τα συστήματα αυτά χρησιμοποιούν κρυπτογράφηση και άλλους μηχανισμούς ασφαλείας για να εξασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στο δίκτυο και ότι τα δεδομένα δεν μπορούν να υποκλαπούν.

3.3.1 Ιδιωτικές και καταναλωτικές VPN υπηρεσίες

Οι χρήστες χρησιμοποιούν μια ιδιωτική υπηρεσία VPN, γνωστή ως σήραγγα VPN, για την προστασία των online δραστηριοτήτων και της ταυτότητά τους. Με τη χρήση μιας υπηρεσίας ανώνυμων VPN, η κυκλοφορία στο Διαδίκτυο ενός χρήστη και τα δεδομένα του παραμένουν κρυπτογραφημένα. Η υπηρεσία αυτή αποτρέπει υποκλοπές δραστηριοτήτων στο Διαδίκτυο. Μια υπηρεσία VPN είναι ιδιαίτερα χρήσιμη κατά την πρόσβαση σε δημόσια Wi-Fi, επειδή η δημόσια ασύρματη υπηρεσία μπορεί να μην είναι ασφαλής. Εκτός από τη δημόσια ασφάλεια των Wi-Fi, μια ιδιωτική υπηρεσία VPN παρέχει επίσης στους χρήστες πρόσβαση στο Internet χωρίς λογοκρισία και μπορεί να βοηθήσει στην πρόληψη της κλοπής δεδομένων και την απεμπλοκή ιστοσελίδων.

3.3.2 Εταιρικές VPN υπηρεσίες

Οι εταιρείες και οι οργανισμοί θα χρησιμοποιήσουν ένα VPN για να επικοινωνήσουν εμπιστευτικά σε ένα δημόσιο δίκτυο και να στείλουν φωνή, βίντεο ή δεδομένα. Είναι επίσης μια εξαιρετική επιλογή για απομακρυσμένους εργαζομένους και των οργανισμών με διεθνή γραφεία και τους συνεργάτες τους να μοιράζονται τα δεδομένα με ιδιωτικό τρόπο.

Ένας από τους πιο κοινούς τύπους των VPNs που χρησιμοποιούνται από τις επιχειρήσεις ονομάζεται εικονικό ιδιωτικό dial-up δίκτυο (VPDN). Ένα VPDN είναι ένας χρήστης-σε-τοπική σύνδεση, όπου οι απομακρυσμένοι χρήστες θέλουν να συνδεθούν με την εταιρεία τοπικά. Ένας άλλος τύπος VPN είναι αυτός που ονομάζεται site-to-site VPN. Εδώ η εταιρεία επενδύει σε ειδικό εξοπλισμό για να συνδέσει πολλούς ιστότοπους στο τοπικό τους δίκτυο μέσω ενός δημόσιου δικτύου, συνήθως το Διαδίκτυο.

Ακολουθούν μερικές από τις πιο δημοφιλείς υπηρεσίες εικονικών δικτύων.

Tunnelbear

Το Tunnelbear [40], προσφέρει 3 ενδιαφέροντα τεχνολογικά χαρακτηριστικά που οι χρήστες θα βρουν χρήσιμα για πρόσθετη προστασία της ιδιωτικής ζωής:

Το "Intellibear" επιτρέπει επιλεκτικά VPN για τις ιστοσελίδες που θέλετε ιδιωτικές, ενώ περιηγείστε χωρίς VPN σε άλλους δικτυακούς τόπους.

Το "Vigilant (Επαγρύπνηση)" είναι μια ασφαλιστική δικλείδα κατά των μικρών παράθυρων όταν εκτίθεσαι σε wi-fi ή σε πτώση σύνδεσης VPN. Η Vigilant θα μπλοκάρει τις μεταδόσεις μέχρι το wi-fi ή μέχρι η σύνδεση VPN αποκατασταθεί.

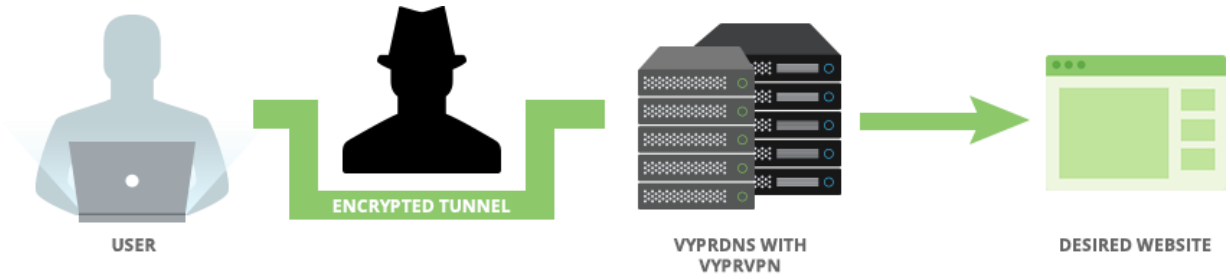
Το "Maul Trackers" προσφέρει μια ενημερωμένη μαύρη λίστα γνωστών ανιχνευτών από τη στιγμή που θα δει το σήμα σας.

VyprDNS - Encrypted, Zero Logging DNS

Οι χρήστες του Διαδικτύου συνήθως βασίζονται σε δικούς τους ISP διακομιστές DNS ή σ' ένα 3ο τμήμα DNS, το οποίο συχνά ρυθμίζεται για την σύνδεση στην διαδικτυακή δραστηριότητα στο διαδίκτυο και λογοκρίνει ιστοσελίδες ακόμα και αν χρησιμοποιείτε ένα VPN.

Το VyprDNS είναι της Golden Frog's [37]μια υπηρεσία που διατίθεται αποκλειστικά στους χρήστες του VyprVPN. Η VyprDNS υπηρεσία δημιουργήθηκε για την αύξηση της προστασία της ιδιωτικής ζωής των χρηστών και για να καταπολεμήσει τη λογοκρισία σε όλο τον κόσμο. Το VyprDNS περιλαμβάνεται με όλα τα προγράμματα και είναι ενεργό κάθε φορά που χρησιμοποιείτε το VyprVPN.

Χρησιμοποιώντας το VyprVPN με το VyprDNS, τα δεδομένα και οι DNS αιτήσεις περνούν μέσα από μια κρυπτογραφημένη σήραγγα που καταργεί τις επιθέσεις των μεσαζόντων DNS και εμποδίζει το φιλτράρισμα DNS ώστε να μπορείτε να βιώσετε μια εμπειρία ανοιχτού internet, όπως φαίνεται στην παρακάτω εικόνα.



PureVPN

Το PureVPN [38] έχει κερδίσει την αγάπη πολλών χρηστών, λόγω του φιλικού λογισμικού για τον πελάτη και την πολύ οικονομική τιμή. Μπορείτε να διαιρέσετε τη σήραγγα, η οποία είναι χρήσιμη για την κρυπτογράφηση συγκεκριμένων συνηθειών των χρηστών στο web, ενώ εξακολουθούν να χρησιμοποιούν την κανονική σύνδεση του δικτύου σας για τους άλλους. Το PureVPN κάνει χρήση του εύρους ζώνης καταγραφής και τη διάρκεια σύνδεσής σας, αλλά διαγράφει αυτές τις πληροφορίες κάθε 5 ημέρες. Οι ταχύτητες για το Pure VPN είναι στα 4 Mbps έως 21 Mbps εύρος, το οποία κατά μέσο όρο είναι πιο γρήγορο από τα περισσότερα άλλα VPN.

Το PureVPN προσφέρει 5 ταυτόχρονα logins, έτσι ώστε να μπορείτε να προστατεύετε την επιφάνεια εργασίας του υπολογιστή σας, του Mac, του φορητού υπολογιστή, του smartphone και του tablet με ένα μόνο λογαριασμό.

Το δίκτυο PureVPN αποτελείται από πάνω από 300 διακομιστές σε όλες τις ηπείρους, που συνδυάζονται για να παρέχουν συνεχή και αδιάκοπη συνδεσιμότητα από όλες τις γωνιές του κόσμου.

3.4 Διακομιστές μεσολάβησης (proxy server)

Βασικά, ένας διακομιστής μεσολάβησης είναι μια point - to - point σύνδεση ανάμεσα σε εσάς και μια απομακρυσμένη τοποθεσία του Διαδικτύου. Αν για παράδειγμα, είστε σ' ένα ξενοδοχείο στη Καλαμάτα και εργάζεστε για μια μεγάλη εταιρεία στην Αθήνα, ανοίγοντας ένα VPN με το εταιρικό γραφείο σας, σημαίνει ότι ο υπολογιστής σας θα δημιουργήσει μια μόνιμη σύνδεση μεταξύ του δικού σας συστήματος και μια ειδική συσκευή στο εταιρικό γραφείο που ονομάζεται VPN server.

Αυτή η σύνδεση σας παρέχει μια σήραγγα μέσα από την οποία όλες οι επικοινωνίες θα περνούν, αυτή είναι η πρώτη και πιο γνωστή ποιότητα ενός VPN. Ότι κυκλοφορεί, θα κρυπτογραφείτε μέσα σε αυτή τη σήραγγα, θα πηγαίνει από την τρέχουσα θέση σας στον VPN server και στη συνέχεια θα δυσανασχετούν για λογαριασμό σας στο ευρύτερο Διαδίκτυο. Αυτό σημαίνει ότι όποιος προσπαθήσει να ακούσει ή προσπαθήσει να δει τα πακέτα που φεύγουν από το δικό σας σύστημα, δεν θα δει τίποτα παρά στατικότητα. Στην πραγματικότητα, δεν θα ξέρουν ποιες ιστοσελίδες επισκέπτεστε, γιατί τα πάντα είναι κρυπτογραφημένα. Αυτός είναι ένας ακόμη πιο ισχυρός μηχανισμό ασφαλείας από το SSL, αφού με το SSL μπορούν κάποιοι να εξακολουθούν να βλέπουν επικεφαλίδες και να γνωρίζουν σε ποιες ιστοσελίδες περιηγείστε.

Αλλά ένα VPN, ή οποιοδήποτε άλλο είδος διακομιστή μεσολάβησης, παρέχει ακόμη περισσότερα οφέλη. Είτε χρησιμοποιήσετε ένα VPN, το οποίο βασίζεται σε ένα πρωτόκολλο όπως το PPTP για να εμπεριέχει τα πακέτα σας με ασφάλεια, είτε ένα SSL διακομιστή μεσολάβησης, είτε ένα Socks διακομιστής μεσολάβησης ή ακόμα και μια απλή πύλη web (που δεν σας παρέχει καμία κρυπτογράφηση), όλα αυτά έχουν χαρακτηριστικά που είναι παρόμοια.

Η βασική αρχή είναι ότι ο διακομιστής αναμεταδίδει αυτά τα πακέτα για χάρη σας και αφαιρεί τη διεύθυνση προέλευσης. Αντί για τη δική σας IP διεύθυνση, βλέπουν την IP του διακομιστή μεσολάβησης. Αυτό σημαίνει, χρησιμοποιώντας το προηγούμενο παράδειγμα, αντί να σκεφτόμαστε ότι είστε στη Καλαμάτα, με όποιο ιστότοπο και να συνδεθείτε θα φαίνετε ότι είστε στην Αθήνα στο εταιρικό σας γραφείο.

Φυσικά, οι άνθρωποι χρησιμοποιούν διαμεσολαβητές και για άλλους λόγους. Ένα παράδειγμα είναι η προσπάθεια να αποκτήσουμε πρόσβαση σε μια περιοχή με περιορισμένο περιεχόμενο. Για παράδειγμα, κάποιος στον Καναδά προσπαθεί να δει περιεχόμενό της Hulu αλλά δεν μπορεί,

επειδή η Hulu βάζει περιορισμούς ώστε τα βίντεο να τα βλέπουν μόνο χρήστες των ΗΠΑ. Αλλά αν αυτοί συνδεθούν με ένα διακομιστή μεσολάβησης που έχει τη βάση του στις ΗΠΑ, μπορούν να παρακάμψουν αυτόν τον περιορισμό. Το ίδιο ισχύει και αν ζείτε στις ΗΠΑ και θέλετε να δείτε το περιεχόμενο του BBC μέσω του iPlayer. Θα πρέπει να συνδεθείτε με ένα διακομιστή μεσολάβησης του Ηνωμένου Βασιλείου για να το πετύχετε αυτό.

Επίσης, οι εγκληματίες χρησιμοποιούν πολύ τους διακομιστές μεσολάβησης για να κρύψουν που βρίσκονται πραγματικά. Μπορούν να δημιουργήσουν μια αλυσίδα από διακομιστές μεσολάβησης για να αυξήσουν τη δυσκολία να τους εντοπίσουν. Αλλά οι διακομιστές μεσολάβησης χρησιμοποιούνται για πολύ περισσότερα από ό, τι για να διαπράξουν κάποιοι εγκλήματα. Πολλοί άνθρωποι τα χρησιμοποιούν μόνο για ασφάλεια.

Αν έχετε μια αργή σύνδεση στο Διαδίκτυο, μπορείτε να χρησιμοποιήσετε ένα διακομιστή μεσολάβησης με μεγάλο εύρος ζώνης. Τα κακόβουλα λογισμικά που κυκλοφορούν στο διαδίκτυο προσπαθούν να βρουν μη ενημερωμένα συστήματα ή ξεκινούν δυναμική άρνηση σε επιθέσεις των υπηρεσιών, θα βρουν μόνο το διακομιστή μεσολάβησης. Οι ερευνητές ασφαλείας επίσης αγαπούν τους διακομιστές μεσολάβησης. Όταν προσπαθείτε να διεισδύσετε στο υπόγειο έγκλημα, το τελευταίο πράγμα που θέλετε είναι να τους δώσετε είναι η διεύθυνση του σπιτιού σας.

3.4.1 Οι διακομιστές μεσολάβησης απαιτούν εμπιστοσύνη

Υπάρχουν μερικά πράγματα που πρέπει να έχετε κατά νου όταν χρησιμοποιείτε διακομιστές μεσολάβησης. Πρώτον, να θυμάστε ότι, ενώ ένας διακομιστής μεσολάβησης σας παρέχει ασφάλεια και ανωνυμία, ο ίδιος ο διαμεσολαβητής έχει αποκωδικοποιήσει όλες τις κινήσεις σας. Αυτό σημαίνει ότι μπορεί να δει οτιδήποτε κάνετε, εκτός και αν χρησιμοποιείτε συνδέσεις SSL. Οπότε πρέπει να τον εμπιστεύεστε. Πολλά άτομα χρησιμοποιούν το TOR, το οποίο είναι ένα δωρεάν δίκτυο ανωνυμίας και τρέχει από εθελοντές, ή κάποιοι προχωρούν σε υπόγεια κανάλια με "ιδιωτικούς" διακομιστές μεσολάβησης, αλλά το πρόβλημα είναι ότι ποτέ δεν ξέρεις αν μπορείς να εμπιστευτείς αυτούς τους servers.

Μπορεί να καταλήξει να είναι χειρότερο από το να μη χρησιμοποιείς καθόλου διακομιστή μεσολάβησης. Δημοφιλή εμπορική υπηρεσία όπως το Hide My Ass βασίζεται στην παροχή αυτής της υπηρεσίας. Σημειώνουμε ότι δεν μπορείτε να χρησιμοποιήσετε αυτές τις εφαρμογές για παράνομες πράξεις, διότι αναφέρουν ρητά ότι συνεργάζονται με τις αρχές επιβολής του νόμου και ο διακομιστής μεσολάβησης είναι ο μοναδικός που ξέρει ποια είναι η πραγματική IP διεύθυνση σας.

Επίσης, χρησιμοποιώντας διακομιστές μεσολάβησης θα επιβραδυνθεί η σύνδεσή σας, επειδή ουσιαστικά μεταφέρει όλα τα δεδομένα σας σε άλλες τοποθεσίες σε όλο τον κόσμο προτού να βγει στο Διαδίκτυο. Αν επιχειρήσετε να συνδεθείτε σε διάφορους proxy servers, θα βρείτε πολύ μεγάλες διαφορές στην ταχύτητα, γι 'αυτό είναι καλή ιδέα να τους δοκιμάζετε. Είτε θέλετε ασφάλεια είτε ανωνυμία, ή και τα δύο, οι διακομιστές μεσολάβησης παρέχουν έναν καλό τρόπο για να περιηγηθείτε στο διαδίκτυο.

3.4.2 Διαφορά μεταξύ διακομιστών διαμεσολάβησης και VPNs

Οι διακομιστές μεσολάβησης και τα VPNs, χρησιμοποιούνται για την προστασία της ασφάλειας των δεδομένων όταν είστε online. Ο τρόπος που γίνεται αυτό, είναι η διαφορά μεταξύ των δύο υπηρεσιών. Μια υπηρεσία με διακομιστή μεσολάβησης δεν προσφέρει κρυπτογράφηση των δεδομένων. Κρυπτογράφηση, όπως των 128-bit και των 256-bit χρησιμοποιούν πολύπλοκους αλγόριθμους για να μπερδέψουν τα στοιχεία σας και να τα καταστήσουν δυσανάγνωστα για επίδοξους hackers και κάθε είδους απειλές.

Τις καλύτερες υπηρεσίες μεσολάβησης, προσφέρουν και οι δύο μαζί, διακομιστές μεσολάβησης και VPN υπηρεσίες. Και οι δύο εργάζονται εξαιρετικά καλά μεταξύ τους: ο proxy σας επιτρέπει να έχετε πρόσβαση σε ιστοσελίδες γρήγορα και ανώνυμα, ενώ ένα VPN κρυπτογραφεί και ασφαλίζει τα στοιχεία σας ώστε να μην είστε ευάλωτοι σε επιθέσεις.

Κεφάλαιο 4
Προστασία της Ιδιωτικότητας στα Δίκτυα Κοινωνικής Δικτύωσης

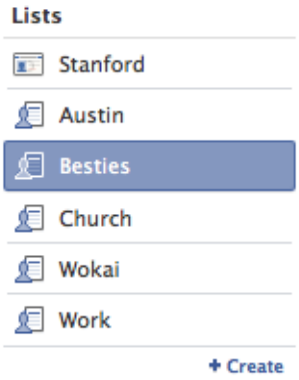
Ενώ σε προηγούμενο κεφάλαιο εξετάσαμε τις δυνατότητες που παρέχουν τα PET για προστασία της Ιδιωτικότητας γενικά και στην πλοήγηση στο διαδίκτυο, στο παρόν κεφάλαιο θα παρουσιάσουμε τις δυνατότητες για προστασία της Ιδιωτικότητας που περιέχουν τα ίδια τα δίκτυα κοινωνικής δικτύωσης. Φυσικά θα αναφερθούμε στα κυριότερα και πιο δημοφιλή, δηλαδή το Facebook, Google+ και το Twitter.

Ακολούθως θα αναφερθούμε σε προτεινόμενες αρχιτεκτονικές δικτύων κοινωνικής δικτύωσης, οι οποίες λαμβάνουν στο σχεδιασμό και την δομή τους την προστασία των προσωπικών δεδομένων. Στο τέλος του κεφαλαίου θα αναφερθούμε στο Diaspora*, το οποίο είναι ένα

παράδειγμα δικτύου κοινωνικής δικτύωσης το οποίο είναι σχεδιασμένο με βάση την προστασία των προσωπικών δεδομένων και τη χρήση τεχνικών προστασίας της Ιδιωτικότητας.

4.1 Facebook

Το Facebook επιτρέπει στους χρήστες του να προσαρμόσουν τις ρυθμίσεις του απορρήτου τους από μια σειρά επιλογών, αλλά ένα εκπληκτικά μικρό ποσοστό των χρηστών διαχειρίζεται ενεργά τις ρυθμίσεις του απορρήτου του. Πολλοί χρήστες που διαμαρτύρονται για την έλλειψη της προστασίας της ιδιωτικής ζωής στο Facebook δεν γνωρίζουν για τις ρυθμίσεις που είναι διαθέσιμες σε αυτούς. Παρακάτω, παρουσιάζονται όλα τα βήματα που πρέπει να ξέρετε για την προστασία της ιδιωτικής ζωής σας στο Facebook.

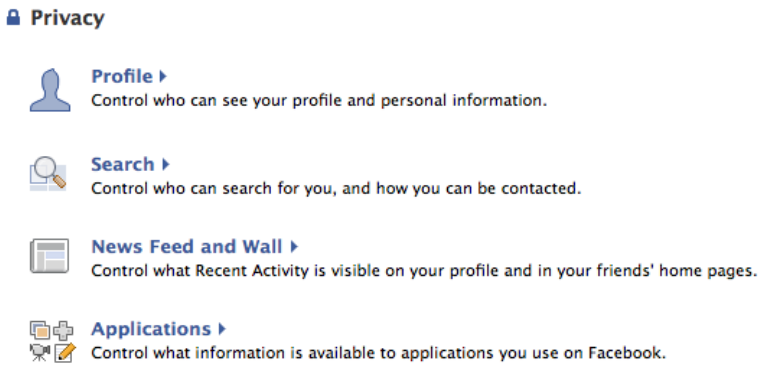


Κάνοντας κλικ στο "Friends" στην κορυφή του μενού σε φέρνει στη σελίδα Friends, όπου μπορείς να δημιουργήσεις λίστες φίλων. Τις λίστες τις οργανώνεις όπως εσύ θέλεις, γεωγραφική περιοχή, είδος σχέσης κ.α. Οι πιο αποτελεσματικές λίστες που δημιουργούνται είναι για δύο κύριες ομάδες φίλων: Αυτούς που σχεδιάζετε να βλέπουν τα πάντα και αυτούς με τους οποίους θα μοιράζεστε πληροφορίες πολύ χαμηλού επιπέδου.

Ρυθμίσεις απορρήτου Dashboard

Για να αποκτήσετε πρόσβαση στις ρυθμίσεις του απορρήτου σας στο Facebook, κάντε κλικ στο "Ρυθμίσεις" στην επάνω γραμμή μενού και στη συνέχεια επιλέξτε "Ρυθμίσεις Απορρήτου" στο

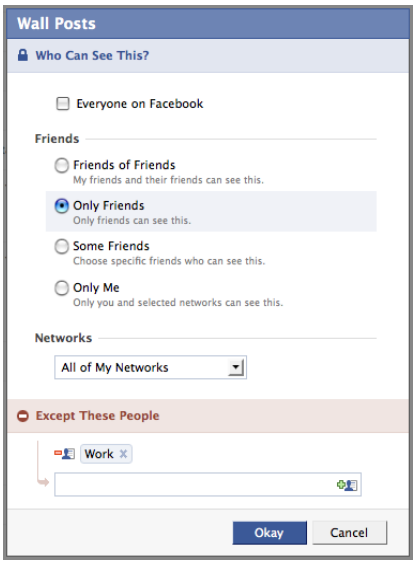
προκύπτον drop-down. Θα εμφανιστεί μια σελίδα όπου μπορείτε να δείτε το παρακάτω μενού επιλογών προστασίας προσωπικών δεδομένων:



Επιλογές Ρυθμίσεων απορρήτου για τον τοίχο σας

Ο τοίχος του Facebook περιέχει πολλές προσωπικές πληροφορίες για τον καθένα, οπότε είναι σημαντικό να σκεφτούμε σε ποιους θέλουμε να δώσουμε πρόσβαση.

Κάποιος απενεργοποίησε τον τοίχο του γιατί ένας φίλος του έγραψε στον τοίχο του για μία θέση εργασίας η οποία δεν είχε ακόμη ανακοινωθεί. Το να κλείσεις τον τοίχο σου (επιλέξτε "Μόνο εγώ") είναι μια επιλογή, μπορείτε να αποφύγετε τέτοιες επικίνδυνες καταστάσεις με πιο ανώδυνο τρόπο, απλά με τον αποκλεισμό συγκεκριμένων φίλων να βλέπουν τον τοίχο σας. Παρακάτω φαίνεται ότι έχετε τη δυνατότητα όλοι οι φίλοι σας να βλέπουν τον τοίχο σας, εκτός από εκείνους στη λίστα Εργασίας σας:

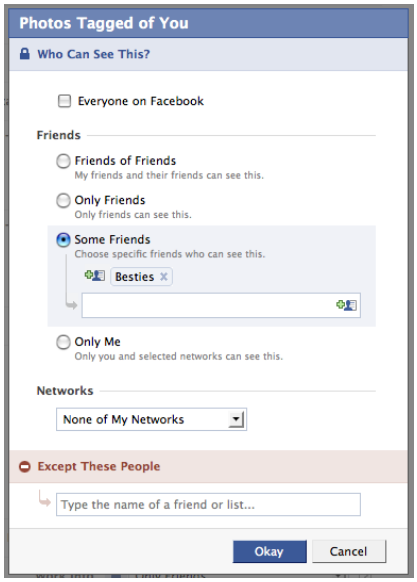


Επιλογή Ρυθμίσεων απορρήτου για τις φωτογραφίες

Υπάρχουν ρυθμίσεις και για τις φωτογραφίες στις οποίες έχετε επισημανθεί, σε περίπτωση που δεν αισθάνεστε άνετα δίνοντας σε κάποιους φίλους σας το δικαίωμα να τις δούνε, αυτό μπορείτε να το κάνετε να συμβεί επιλέγοντας, μόνο οι φίλοι της λίστας Besties να έχουν πρόσβαση σε φωτογραφίες που έχετε επισημανθεί.

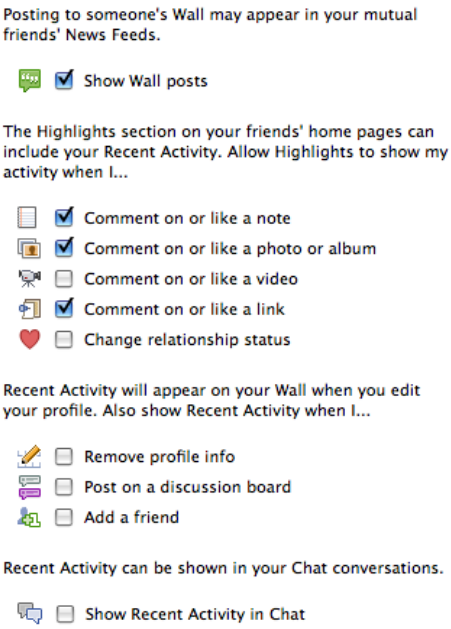
Η παραπάνω ρύθμιση ισχύει μόνο για φωτογραφίες που έχετε επισημανθεί, όχι για τα άλμπουμ φωτογραφιών που έχετε δημιουργήσει. Για να επεξεργαστείτε τα άλμπουμ, μεταβείτε στην καρτέλα Φωτογραφίες από το προφίλ σας και κάντε κλικ στο σύνδεσμο "Album Privacy" στο κάτω μέρος.

Σε περίπτωση αμφιβολίας, μπορείτε να δείτε το δικό σας προφίλ από τη θέση κάποιου φίλου σας. Μπορείτε επίσης να αποκλείσετε ένα φίλο: αυτό ισοδυναμεί με προσωρινή απομάκρυνση των φωτογραφιών, που σημαίνει ότι ο συγκεκριμένος φίλος δεν μπορεί να τις βλέπει.



Επιλέγοντας τι είδους News Feed Stories μπορούν να δουν οι άλλοι για σένα

Μπορείτε να προσδιορίσετε ποιες από τις ενέργειές σας θα δημοσιεύονται στο News Feed και το δικό σας τοίχο, με την προσαρμογή των Πρόσφατων ρυθμίσεων δραστηριοτήτων. Με την ανοιχτή διαδικασία επικοινωνίας API του Facebook, είναι λογικό να αφήνετε τα δημοσιεύματα του τοίχου σας να εμφανίζονται στους φίλους σας, να εμφανίζονται σε κοινούς φίλους News Feeds, ενώ η αλλαγή κατάστασης της σχέσης σας μπορεί να μην θέλετε να μεταδοθεί.



Επιλογές για το τι θέλεις να εμφανίζεται στο Facebook's Social Ads

Επιπλέον, μπορείτε να επιλέξετε αν θέλετε ή όχι να εμφανίζονται στο Social Ads, οι διαφημίσεις του Facebook που έχετε αλληλεπιδράσει να τις βλέπουν οι φίλοι σας.

Επιλογές για το ποιος μπορεί να δει, ποια πεδία από τις πληροφορίες του προφίλ σας.

Στις ρυθμίσεις απορρήτου του προφίλ, τα ακόλουθα πεδία στην καρτέλα Πληροφορίες του προφίλ σας είναι υπό τον έλεγχό σας:

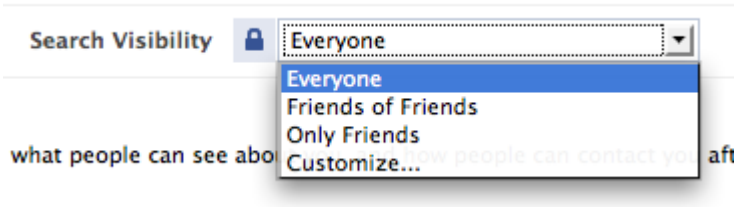
Basic	Contact
Profile	IM Screen Name
Basic Info	Mobile Phone
Personal Info	Other Phone
Status and Links	Current Address
Photos Tagged	Website
Videos Tagged	Residence
Wall Posts	Email
Education Info	
Work Info	

Μπορείτε να επιλέξετε ποιος μπορεί να δει κάθε ένα από αυτά τα πεδία του προφίλ σας με βάση τις λίστες των φίλων, ακριβώς όπως μπορείτε και στον τοίχο σας. Δεν θέλετε οι άνθρωποι που συναντήσατε σε συνέδρια ή πάρτυ να γνωρίζουν τον αριθμό τηλεφώνου σας; Επιτρέψτε να είναι ορατό μόνο στους καλύτερους φίλους σας.

Επιλέγοντας πώς θέλετε να εμφανίζεστε στις αναζητήσεις του Facebook

Η ενότητα Ρυθμίσεις αναζήτησης της ιδιωτικής ζωής είναι εκεί όπου μπορείτε να διασφαλίσετε τον τρόπο με τον οποίο θα σας βρίσκουν οι άνθρωποι που ψάχνουν για σας, τόσο μέσα όσο και έξω από το Facebook.

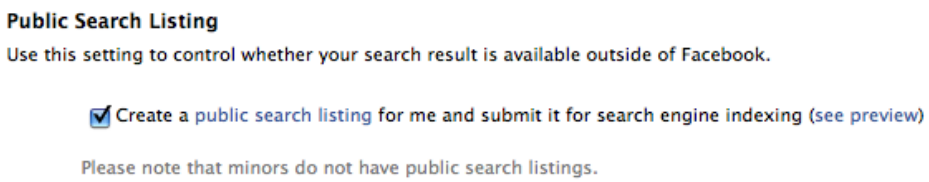
Μέσα στο Facebook, είτε ο καθένας, είτε από κοινούς φίλους, ή μόνο οι φίλοι μπορούν να αναζητήσουν για εσάς, ανάλογα με το πώς έχετε ορίσει τις ρυθμίσεις αναζήτησης. Στη συνέχεια μπορείτε να αποφασίσετε ποιες πληροφορίες θέλετε να συμπεριληφθούν στα αποτελέσματα αναζήτησης (φωτογραφίες, φίλοι, συνδέσεις για να σας προσθέσει ως φίλο / στείλτε ένα μήνυμα, ιστοσελίδες που είστε οπαδοί).



Επιλέγοντας πώς θέλετε να εμφανίζεστε στις αναζητήσεις της Google

Έξω από το Facebook, μπορείτε να δώσετε άδεια στο Facebook να δημιουργήσει μια δημόσια λίστα αναζήτησης του προφίλ σας, ή μπορείτε να επιλέξετε να μη γίνεται αυτό απλά καταργώντας την επιλογή "Δημιούργησε μια δημόσια λίστα αναζήτησης του προφίλ μου".

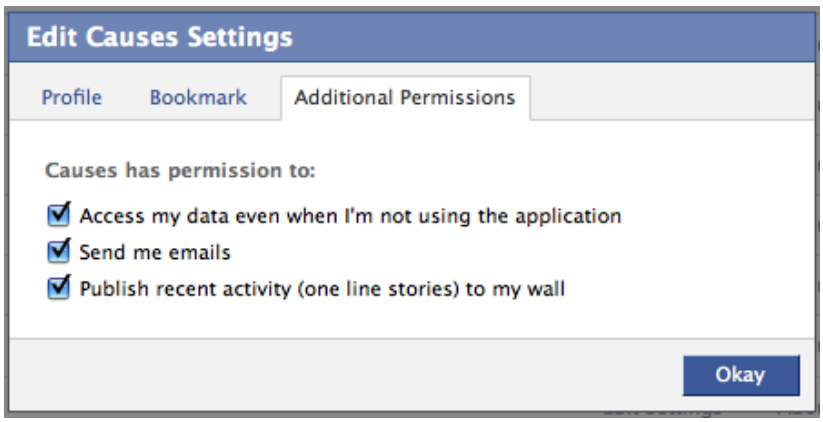
Πολλοί χρήστες δεν γνωρίζουν ότι αυτό το πλαίσιο επιλέγεται αυτόματα, που σημαίνει ότι αυτά που είναι διαθέσιμα για όλους εμφανίζονται στη μηχανή αναζήτησης της Google - γεγονός που σημαίνει ότι ο καθένας μπορεί να βρει το όνομά σας, τη φωτογραφία του προφίλ σας και άλλες βασικές πληροφορίες για εσάς, όπως σελίδες που είστε οπαδοί στο Facebook.



Επιλογές ρυθμίσεων απορρήτου Εφαρμογών

Το Facebook ξεκαθαρίζει κάθε φορά που έχετε δικαίωμα να χρησιμοποιήσετε εφαρμογές να έχουν πρόσβαση στα προσωπικά σας δεδομένα . Θα σας εμφανίζετε πάντα ένα αυτόματο μήνυμα σε παράθυρο για να επιλέξετε αν θέλετε ή όχι να επιτραπεί σε μια εφαρμογή να έχει πρόσβαση στο προφίλ σας.

Για να αλλάξετε τις ρυθμίσεις των εφαρμογών σας, βρείτε το αρχικό μενού των εφαρμογών στην κάτω αριστερή γωνία και κάντε κλικ στο κουμπί "Επεξεργασία". Για κάθε εφαρμογή, θα μπορείτε να επιτρέπετε (ή να απαγορεύετε) στην εφαρμογή πρόσβαση στα δεδομένα / στα απεσταλμένα μηνύματα ηλεκτρονικού ταχυδρομείου / στις δημοσιεύσεις του τοίχου σας , καθώς και ποιος μπορεί να δει την εφαρμογή στο προφίλ σας, εάν φυσικά καταργήσετε την κατάλληλη επιλογή.



4.2 Google+

Το Google+ είναι το νέο κοινωνικό δίκτυο και ένας από τους κύριους λόγους που τόσοι πολλοί άνθρωποι ενδιαφέρονται για την υπηρεσία αυτή παραπάνω από το Facebook είναι ότι εστιάζει στην προστασία της ιδιωτικής ζωής των χρηστών του. Είτε είστε νέος χρήστης του Google+ είτε είστε ήδη έμπειρος, η κατανόηση πώς να ελέγχετε τις πληροφορίες σας στο κοινωνικό δίκτυο μπορεί να σας κάνει να αισθανθείτε πολύ πιο άνετα.

Απόρρητο και οι κύκλοι σας

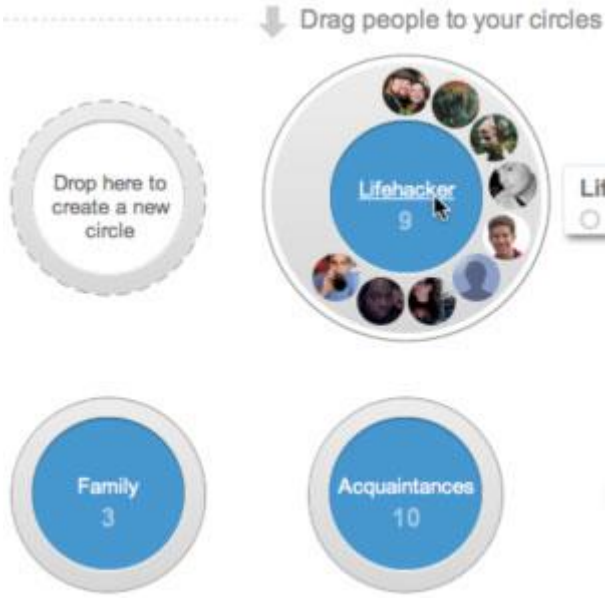
Οι κύκλοι του Google+ αποτελούν ένα εύκολο τρόπο για την οργάνωση των επαφών σας. Οι περισσότεροι έλεγχοι της ιδιωτικής ζωής θα προέλθουν από το πώς έχετε ρυθμίσει τους κύκλους σας, δεδομένου ότι μπορείτε να ορίσετε ρυθμίσεις ελέγχου της ιδιωτικής σας ζωής και για τα δημοσιεύματα και για τις πληροφορίες του προφίλ σας στις ομάδες που έχετε φτιάξει. Βασικά, μπορείτε να δημιουργήσετε έναν κύκλο, όπως “Οικογένεια”, “Εργασία”, “Tech Bloggers”, κλπ. και

να σέρνετε μέσα σε αυτούς τους ανθρώπους που θέλετε να μοιραστείτε τις πληροφορίες ή τίνος τα δημοσιεύματα θέλετε να ακολουθείτε σε αυτές τις ομάδες

Πράγματα που πρέπει να ξέρετε:

- Οι κύκλοι σας είναι προστατευμένοι από την αρχή (από προεπιλογή). Οι κύκλοι σας δημιουργούνται από εσάς και ποιοι θα είναι σε αυτούς τους κύκλους το γνωρίζετε μόνο εσείς. Οπότε, μπορείτε να δημιουργήσετε ένα κύκλο με το όνομα "Lunatics" δηλαδή ανισόρροποι, και να βάλετε μέσα το αφεντικό σας και άλλους που θεωρείτε ανισόρροπους.

- Η Διαχείριση του, ποιος βλέπει ποιες δημοσιεύσεις μπορεί να είναι δύσκολο με αυτό το σύστημα. Το κύριο ζήτημα και πιο σημαντικό είναι να θυμάστε ποιους έχετε βάλει σε ποιους κύκλους. Θα μπορούσατε, σκόπιμα να έχετε τοποθετήσει το αφεντικό σας στον κύκλο Lunatics αλλά και στον κύκλο Εργασία, οπότε θα πρέπει να θυμάστε σε ποιους κύκλους τους έχετε τοποθετήσει. Θα πρέπει να είστε προσεκτικοί με την επιλογή των κύκλων για να μοιραστείτε δημοσιεύσεις.



Διαφορές μεταξύ των κύκλων της Google+, τους οπαδούς του Twitter ή τους φίλους στο Facebook

Πολλοί άνθρωποι, θεωρούν ότι είναι πολύ έξυπνο και βασικό να χρησιμοποιείς κύκλους. Είναι πιο ξεκάθαρο και σαφές από τις λίστες των φίλων του Facebook, αλλά υπάρχει και μια δυσκολία να θυμάστε πώς λειτουργούν οι κύκλοι, ειδικά αν έχετε συνηθίσει να χρησιμοποιείτε το Twitter και το Facebook:

- Όπως με το Twitter, μπορείτε να ακολουθείτε τις δημοσιεύσεις οποιουδήποτε, στο Google+ με την προσθήκη κάποιου σε έναν από τους κύκλους σας - χωρίς το πρόσωπο αυτό να χρειάζεται να σας ακολουθήσει. Δεν είναι το μοντέλο φιλίας ένας-προς-ένας, όπως το Facebook, δηλαδή να πρέπει να θέλουν και οι δύο για να γίνουν φίλοι. Υπό αυτή την έννοια, είναι πολύ περισσότερο όπως το Twitter.

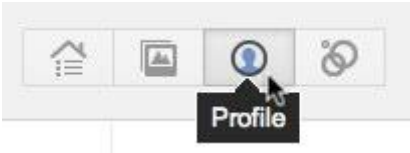
- Από την άλλη πλευρά, ο καθένας μπορεί να σας προσθέσει στους κύκλους του χωρίς τη συγκατάθεσή σας, σε αντίθεση με το Twitter που έχεις την επιλογή "Προστατέψτε τα tweets μου", στο Google+ δεν υπάρχει ρύθμιση που να απαιτεί την έγκρισή σας για να σας ακολουθήσουν άλλοι. Το βάρος πέφτει σε σας να επιλέξετε τις σωστές ρυθμίσεις για τις δημοσιεύσεις σας. Ακόμα κι αν κάποιος σας ακολουθεί αλλά εσείς δεν θέλετε, δεν πρόκειται ποτέ να δει καμιά από τις δημοσιεύσεις σας για όσο διάστημα δεν δημοσιεύετε πληροφορίες σε όλο το κοινό.

Λοιπόν, από τη μία πλευρά, οι κύκλοι του Google+ είναι πολύ πιο απλό να στηθούν και να χρησιμοποιηθούν, επειδή αποτελούν τη βάση αυτού του μοντέλου κοινωνικής δικτύωσης. Από την άλλη, είναι σαν ένα συνονθύλευμα από άλλα κοινωνικά δίκτυα, το οποίο μπορεί να προκαλέσει σύγχυση στην αρχή.

Αν ο καθένας μπορεί να σε ακολουθήσει ή να σε προσθέσει στους κύκλους του, το σημαντικό που πρέπει να θυμόμαστε είναι ότι η προστασία των δημοσιεύσεων σας καθορίζεται από εσάς. Το Google+ έχει πολλά στοιχεία ελέγχου που επιτρέπουν ποιος μπορεί θα δει τις πληροφορίες του προφίλ σας, αλλά και ποιος μπορεί να δει κάθε δημοσίευση.

Ελέγξτε ποιοι θα μάθουν για σένα από το προφίλ σου

Το προφίλ του Google+ παρουσιάζει το ιστορικό σας (το επάγγελμα, την εκπαίδευση, μέρη που ζήσατε, κλπ.), φωτογραφίες και βίντεο που μοιράζεστε με όλους, καθώς και ιστοσελίδες που έχετε επισκεφθεί από μία φορά και πάνω, από τα αποτελέσματα αναζήτησης της Google. Οπότε, αφού ορίσετε τις κοινωνικές ομάδες σας σε κύκλους, η επεξεργασία της σελίδας του προφίλ του Google+ είναι ένας από τους σημαντικούς τρόπους για να ελέγχετε την ιδιωτική σας ζωής στο Google+.



Για να επεξεργαστείτε τις ρυθμίσεις του προφίλ σας, κάντε κλικ στο κουμπί που μοιάζει με ένα κύκλο και μια σιλουέτα σε αυτό, στη συνέχεια, κάντε κλικ στο κουμπί "Επεξεργασία προφίλ".

Εδώ παρουσιάζονται οι προεπιλεγμένες ρυθμίσεις για τις πληροφορίες του προφίλ σας:

- Ονοματεπώνυμο: Αυτό είναι το μόνο απαιτούμενο μέρος του προφίλ σας και είναι ορατό σε όλους. Αλλάζοντας το όνομά σας εδώ θα αλλάξει το όνομά σας σε όλες τις υπηρεσίες της Google.

- Ο καθένας στο διαδίκτυο μπορεί επίσης να δει: Πότε γίνατε μέλος, τη φωτογραφία του προφίλ σας, το φύλο, ποιοι ανήκουν στους κύκλους σας, ποιους έχετε προσθέσει στους κύκλους σας, και το κουμπί για να σας στείλουν μήνυμα ηλεκτρονικού ταχυδρομείου (αλλά όχι την πραγματική διεύθυνση ηλεκτρονικού ταχυδρομείου σας).

- Οι κύκλοι σας μπορούν να δουν: Πότε γίνατε μέλος, την απασχόληση σας, την εκπαίδευση σας, τα μέρη που ζήσατε, την κατάσταση της σχέσης σας, ενδιαφέροντα, συνδέσμους.

- Κλειδωμένο, μόνο μέχρι να το αλλάξετε: το επάγγελμά σας, τα στοιχεία επικοινωνίας σπιτιού και εργασίας.

- Μπορείτε να αλλάξετε κάθε ένα από αυτά τα τμήματα και να επιτρέπετε την προβολή σε: όλο τον κόσμο (ο καθένας στο διαδίκτυο), σε εκτεταμένους κύκλους, στους κύκλους σας, μόνο σε εσάς, ή σε μια συγκεκριμένη ομάδα. Κάθε ομάδα ρυθμίσεων προστασίας της

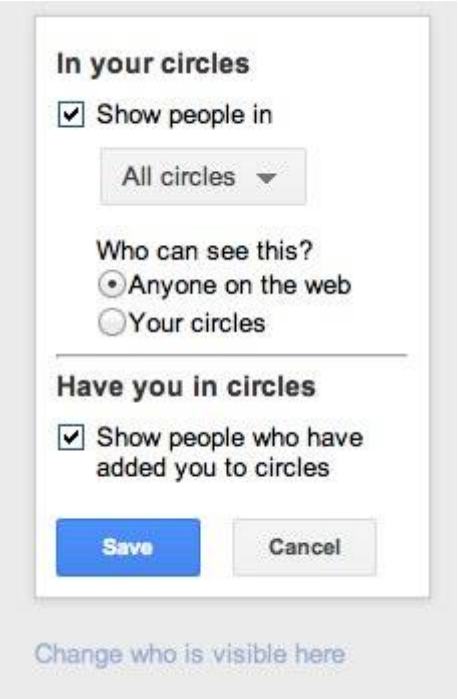
ιδιωτικής ζωής έχει το δικό του εικονίδιο (δείτε την εικόνα στα αριστερά), έτσι ώστε όταν κοιτάτε το προφίλ σας, να μπορείτε να δείτε γρήγορα ποια τμήματα είναι κοινά και σε ποιες ομάδες.

- Έτσι, για παράδειγμα, μπορείτε να ορίσετε το πότε γίνατε μέλος να είναι ορατό στον καθένα στο διαδίκτυο, η απασχόληση σας να είναι ορατή σε όλους που έχετε προσθέσει στους κύκλους σας, τα στοιχεία επικοινωνίας σας να είναι ορατά σε μια συγκεκριμένη επιλογή κύκλων, όπως τους φίλους και την οικογένεια, και η κατάσταση της σχέσης σας να είναι ορατή μόνο σε σας και σε άλλους που είναι σημαντικοί για εσάς, να μπορούν να το δουν.

- Αν θέλετε να ελέγξετε αν το προφίλ σας μοιάζει με κάποιου άλλου, υπάρχει μια επιλογή "Προβολή προφίλ ως ..." πεδίο εισαγωγής στην πάνω δεξιά γωνία στο προφίλ σας, όπου μπορείτε να επιλέξετε.

- Ορατότητα του προφίλ σας στις Αναζητήσεις. Αν δεν θέλετε το προφίλ σας να βρίσκεται στο ευρετήριο της Google και να εμφανίζεται στα αποτελέσματα αναζήτησης, είναι μία ρύθμιση στο κάτω μέρος του προφίλ σας, στο "Σχετικά με τη σελίδα". Καταργήστε την επιλογή "Βοηθείστε τους άλλους να βρίσκουν το προφίλ μου στα αποτελέσματα αναζήτησης" το οποίο είναι επιλεγμένο από προεπιλογή.

- Ποιοι είναι στους κύκλους σας / Σε ποιους κύκλους βρίσκεστε μέσα. Αν είστε στην επεξεργασία της σελίδας του προφίλ σας, μπορείτε επίσης να αλλάξετε την εμφάνιση των ατόμων στο κοινωνικό δίκτυο σας. Κοιτάξτε στην αριστερή στήλη. Κάτω από τις λίστες με τους κύκλους σας, κάντε κλικ στο "Αλλάξτε ποιος είναι ορατός εδώ" για να ελέγχετε ποιος μπορεί να βλέπει όλα τα άτομα που έχετε στους κύκλους σας (δηλαδή, ποιους εσείς ακολουθείτε), καθώς και όλους όσους σας έχουν στους κύκλους τους (οι οποίοι ακολουθούν εσάς).



- Και πάλι, από προεπιλογή, ο καθένας στο διαδίκτυο μπορεί να δει ποιους έχετε προσθέσει στους κύκλους σας και ποιος σας έχει προσθέσει στους δικούς του. Αυτό, όμως, μπορεί να προσαρμοστεί.

- Έχετε επιλογές για να κάνετε τον κόσμο να πιστεύει ότι ακολουθείτε μια συγκεκριμένη ομάδα ή ομάδες ατόμων - αποκλείοντας άλλες ομάδες από την προβολή τους ή κρύβοντας όλα τα άτομα που ακολουθείτε στην πραγματικότητα. Μπορείτε να κρύψετε τον καθένα που σας έχει προσθέσει στους κύκλους του, έτσι ώστε κανείς να μην ξέρει πόσα άτομα ή ποια άτομα σας ακολουθούν.

- Οι φωτογραφίες στο προφίλ, e-mail, σύνδεσμοι. Στο άλλο τμήμα της σελίδας του προφίλ προσαρμόζονται: η κεντρική φωτογραφία και η σειρά των φωτογραφιών του προφίλ σας, ο σύνδεσμος "στείλε ένα e-mail" και οι web σύνδεσμοί σας. Από προεπιλογή, ο καθένας στο διαδίκτυο μπορεί να τα δει αυτά. Εάν αυτό σας ενοχλεί, μπορείτε να το αλλάξετε.

Φωτογραφίες, βίντεο και +1

Οι φωτογραφίες στο προφίλ, τα κοινά άλμπουμ από το Picasa, φωτογραφίες στις οποίες έχετε επισημανθεί από άλλους χρήστες του Google+ και οι άμεσα ανεβασμένες φωτογραφίες, όλες εμφανίζονται εδώ. Μπορείτε να επιλέξετε να μην παρουσιάζετε αυτή η καρτέλα (προβάλλονται από προεπιλογή), αλλά ακόμα κι αν προβάλλεται η καρτέλα των φωτογραφιών σας, μόνο οι φωτογραφίες που μοιράζεστε με άλλους θα εμφανιστούν σε αυτούς.

Μια περίεργη ρύθμιση είναι ότι "Τα άτομα τα οποία σας έχουν επισημάνει σε φωτογραφίες, αυτόματα έχουν την άδεια να συνδεθούν με το προφίλ σας", έχει οριστεί ως προεπιλογή να επιτρέπεται για τους κύκλους σας. Η ρύθμιση αυτή σημαίνει απλά ότι αν κάποιος σε επισημάνει σε μια φωτογραφία και την εγκρίνεις, η φωτογραφία θα συνδέεται αυτόματα με το προφίλ σου και θα προστεθεί και εκεί.

Τη καρτέλα βίντεο έχετε τη δυνατότητα να την αποκρύπτετε ή να την εμφανίζετε. Θα πρέπει υποχρεωτικά να μοιραστείτε τα βίντεο, αλλά η καρτέλα εμφανίζεται από προεπιλογή.

Όταν σας αρέσει μια σελίδα ή μια ιστοσελίδα κάνοντας κλικ στο κουμπί +1 στα αποτελέσματα αναζήτησης ή στην ιστοσελίδα, θα εμφανίζεται στη σελίδα του προφίλ σας, αν έχετε αυτή τη ρύθμιση από προεπιλογή. (Σημείωση: κάνοντας κλικ +1 σε σχόλια για μια δημοσίευση δεν θα εμφανιστεί σε αυτήν την καρτέλα .Θα εμφανίζεται μόνο στη σειρά των σχολίων). Εάν δεν θέλετε οι υπόλοιποι να βλέπουν τα +1 σας, απενεργοποιήστε αυτήν την καρτέλα.

Μοιραστείτε μόνο με επιλεγμένα άτομα που χρησιμοποιούν Κύκλους

Μετά την οργάνωση των ατόμων σε ομάδες για την ανταλλαγή και την προσαρμογή των ρυθμίσεων του προφίλ σας, η επόμενη μεγάλη ανησυχία της προστασίας της ιδιωτικής ζωής είναι ποιος μπορεί να δει και να μοιραστεί το περιεχόμενο που δημοσιεύετε (η οποία μπορεί να περιλαμβάνει μια φωτογραφία, σύνδεση στο διαδίκτυο, βίντεο, χάρτες με τοποθεσία).

Ομάδες με τις οποίες μπορείτε να μοιραστείτε: Όταν μοιράζεστε το περιεχόμενο σας με την υπηρεσία της "ροής", μπορείτε να επιλέξετε ποιοι κύκλοι ή ποια άτομα, θα μπορούν να δουν το περιεχόμενο με την προσθήκη ενός ή περισσότερων από αυτούς στις ομάδες:

- Δημόσια ομάδα: ορατή σε όλους όσους έχετε προσθέσει στους κύκλους σας, εμφανίζεται και στη σελίδα του προφίλ σας.

- Επεκτάσιμοι Κύκλοι: ο καθένας στη Δημόσια ομάδα, καθώς και όλοι στους κύκλους τους, όπως και οι φίλοι των φίλων στο Facebook

- Το όνομα ενός ή περισσότερων από τους Κύκλους σας

- Μεμονωμένα ονόματα των ατόμων στο Google+ (είναι όπως όταν στέλνετε ένα άμεσο μήνυμα σε κάποιον στο Google+. Απλά εισάγετε το όνομά του, ως το πρόσωπο με το οποίο μοιράζεστε την ανάρτηση).

Επιλογή των ομάδων που μοιράζεστε πληροφορίες

Όταν έχετε ορίσει την ομάδα σας και δημοσιεύετε το περιεχόμενό σας, δεν μπορείτε να αλλάξετε την ομάδα με την οποία το μοιράζεστε από κοινού. Για παράδειγμα, τη στιγμή που έχετε ορίσει κάτι δημόσιο για όλες τις επαφές των κύκλων σας, θα είναι εμφανή σε όλους όσους έχετε προσθέσει στους κύκλους σας.

Από προεπιλογή, όταν δημιουργείτε μια νέα ανάρτηση, οι κύκλοι ή τα άτομα με τα οποία μοιραζόσασταν από κοινού τελευταία, θα είναι αυτοί με τους οποίους θα μοιραστείτε την

επόμενη ανάρτηση από προεπιλογή. Αυτό είναι βολικό αν συχνά μοιράζεστε με τις ίδιες ομάδες ή άτομα, αλλά προτείνετε να ελέγχετε συχνά την ρύθμιση "μοιράζομαι με" για κάθε δημοσίευση.

Η κοινή χρήση με τους κύκλους είναι χωρίς αποκλεισμούς, όχι όμως αποκλειστική. Επί του παρόντος, μπορείτε να επιλέξετε μόνο συγκεκριμένες ομάδες που θέλετε να μοιραστείτε το περιεχόμενό σας, δεν μπορείτε να ρυθμίσετε να μοιράζεστε τη δημοσίευση με όλους εκτός από ένα συγκεκριμένο κύκλο ή ένα πρόσωπο. Αυτό σημαίνει ότι αν θέλετε να δημοσιεύσετε αρνητικά σχόλια για το χώρο εργασίας σας, δεν μπορείτε να δημιουργήσετε έναν κύκλο εργασίας και να δημοσιεύσετε κάτι το οποίο να αποκλείει τον κύκλο αυτό. Θα πρέπει να δημιουργηθεί κάτι σαν "όλοι εκτός από την εργασία" για να μοιραστείς άσχημες ιστορίες της εργασίας σου. Ομοίως, αν για παράδειγμα, θέλετε να γράψετε ένα μυστικό, σχετικά με μια έκπληξη γενεθλίων κάποιου φίλου σας στο Google+ και θέλετε να περιλαμβάνονται όλοι εκτός από αυτόν, το Google+ δεν θα επιτρέψει μία τέτοια πράξη.

Έλεγχος των στοιχείων και των δημοσιεύσεων σας

Εκτός από τον καθορισμό ποιοι κύκλοι μπορούν να δουν τις αναρτήσεις σας, υπάρχουν και άλλα διαθέσιμα εργαλεία για τη ρύθμιση των αναρτήσεων (δείτε το μικρό τρίγωνο στην επάνω δεξιά γωνία της κάθε ανάρτησης που κάνετε): Αν έχετε ροδέλες για σύρσιμο σε μία από τις αναρτήσεις σας, μπορείτε να τις αφαιρέσετε μεμονωμένα ή να τις αναφέρετε στη Google. Μπορείτε να απενεργοποιήσετε όλους τους σχολιασμούς (π.χ. αν αυτό είναι ένα θέμα που αφορά την ομάδα σας και απλά θέλετε να το κοινοποιήσετε στην ομάδα σας). Και μπορείτε να απενεργοποιήσετε την αναδημοσίευση. Όλα αυτά πρέπει να γίνουν με το χέρι για κάθε ανάρτηση.

Εισερχόμενες ροές. Αναρτήσεις από τα άτομα που έχετε προσθέσει στους κύκλους σας, θα εμφανιστούν στη "ροή" σε διάφορες κατηγορίες των κύκλων σας.

Τα άτομα που δεν έχετε προσθέσει στους κύκλους σας αλλά που σας ακολουθούν, τις αναρτήσεις τους θα πρέπει να τις μοιραστούν μαζί σας στον "Εισερχόμενο" σύνδεσμο. Μπορείτε να κλείσετε αναρτήσεις που δεν σας ενδιαφέρουν, να μην υπάρχουν εκεί ή να προσθέσετε μερικά από αυτά τα άτομα στους κύκλους σας.

Αποκλεισμός ατόμων. Αν υπάρχουν πάρα πολλά ανεπιθύμητα ή προσβλητικά δημοσιεύματα ή έχετε κατακλυστεί με δημοσιεύσεις από κάποια άτομα, μπορείτε να τους αποκλείσετε στις ρυθμίσεις των κύκλων σας. Το μπλοκάρισμα εδώ, ωστόσο, ενδέχεται να μην λειτουργεί όπως νομίζετε.

Με άλλα λόγια, μη σκεφτείτε ότι αποκλείοντας ένα χρήστη πράγματι προστατεύετε την ιδιωτική σας ζωής.

Τα σχόλια σας σε αναρτήσεις άλλων είναι δημόσια: Σημειώστε ότι τα σχόλια σας σχετικά με θέματα άλλων ατόμων, αν αυτά τα θέματα μοιράζονται σε όλους, είναι και δημόσια και βρίσκονται στο ευρετήριο της Google (δηλαδή, με δυνατότητα αναζήτησης). Τα δικά σας +1 σε δημοσιεύσεις άλλων ατόμων είναι επίσης δημόσια, γι αυτό το λόγο πρέπει να είστε προσεκτικοί. Μια μεμονωμένη ανάρτηση θα είναι "Περιορισμένη" ή "Δημόσια" δίπλα στην ώρα, έτσι θα γνωρίζετε τι μοιράζεστε με έναν κύκλο ή με το ευρύ κοινό.

4.3 Twitter

Εκ πρώτης όψεως το Twitter έχει ίσως την πιο απλή πολιτική προστασίας προσωπικών δεδομένων από κάθε άλλο κοινωνικό δίκτυο:

Είτε ο καθένας μπορεί να διαβάσει τα tweets σας (ό, τι αναφέρετε στο twitter είναι δημόσιο) ή μπορείτε να κάνετε τις πληροφορίες που ανεβάζετε ιδιωτικές (και στη συνέχεια μια λίστα ατόμων να έχουν τη δυνατότητα να τις δουν).

Επίσης, μπορείτε, ανεξάρτητα από την επιλογή που έχετε κάνει, να αποκλείσετε κάποια άτομα ώστε να μη μπορούν να σας ακολουθούν. Ο αποκλεισμός ενός ατόμου δεν είναι εξαιρετικά αποτελεσματική πρακτική, εφ' όσον μπορεί στη συνέχεια να αποσυνδεθεί και να διαβάσει τις πληροφορίες σας που μοιράζεστε δημόσια ούτως ή άλλως, αλλά μπορεί να περιοριστεί ως spam.

Αναδημοσίευση (retweet)

Μπλοκάροντας όλους όσους δεν ξέρετε δεν είναι η λύση του προβλήματος. Ακριβώς όπως το κουτσομπολιό, όποιος μπορεί να διαβάσει τι έχετε πει μπορεί και να το μοιραστεί. Είναι αρκετά συχνό στο twitter το "retweet", η αναδημοσίευση ενός μηνύματος: δηλαδή, επανάληψη του μηνύματος αυτολεξεί ή μερικές φορές με μικρές αλλαγές στο μήκος ή τη προσθήκη σχολίων.

Όταν έχετε ένα δημόσιο λογαριασμό, η αναδημοσίευση είναι η πιο ακίνδυνη συμπεριφορά. Ο καθένας αν κοιτάξει μπορεί να δει εκείνο το αστείο που είπατε, έτσι ώστε αν ένας από τους οπαδούς σας το αναδημοσιεύσει, τότε ακόμη περισσότεροι άγνωστοι μπορούν να το δουν. Θα μπορούσαν να δουν αυτό το tweet ανά πάσα στιγμή, εάν το επιθυμούσαν.

Ωστόσο, η ιστορία μπορεί να είναι αρκετά διαφορετική, αν έχετε ένα ιδιωτικό λογαριασμό. Ίσως αν επιλέξετε να διατηρήσετε το λογαριασμό σας ιδιωτικό, επειδή εσείς και το αφεντικό σας δεν μοιράζεστε τις πολιτικές σας απόψεις. Αυτό το "αστείο" που είπατε θα μπορούσε να σας φέρει σε δύσκολη θέση αν τελικά το δει από κάποιον άλλο που το αναδημοσίευσε. Πιθανώς έχετε επιλέξει να κάνετε το λογαριασμό σας ιδιωτικό για κάποιο λόγο, και οι αναδημοσιεύσεις μπορεί να παραβιάσουν την προσδοκία σας για ιδιωτική ζωή.

Παραβίαση της ιδιωτικής ζωής λόγω αναδημοσιεύσεων

Για το θέμα αυτό υπάρχει μία μελέτη των Meeder et al (2010) [20] , όπου διαπιστώθηκε ότι ενώ ορισμένοι πελάτες έκαναν αποκλεισμό σε κάποιους χρήστες για να μην αναδημοσιεύουν ιδιωτικές πληροφορίες, πολλοί όμως δεν το έκαναν και οι χρήστες μπορούσαν απλά πληκτρολογώντας RT και επαναλαμβάνοντας ολόκληρο το μήνυμα να αναδημοσιεύουν.

Ερευνητές συνέλεξαν 4.420.000 tweets που εκθέτουν προσωπικές πληροφορίες με αυτόν τον τρόπο και αναμένουν ότι οι αριθμοί θα συνεχίσουν να ανεβαίνουν.

Δεν γνωρίζουμε, αν αυτά τα εκατομμύρια εκτεθειμένα tweets ήταν προβληματικά για τους ανθρώπους που εκτέθηκαν. Ίσως εκατομμύρια άτομα να ρωτήθηκαν πριν τα αναδημοσιεύσουν (κάτι που πρέπει πάντα να κάνετε πριν δημοσιεύσετε προσωπικές πληροφορίες άλλων). Ίσως τα περισσότεροι tweets ήταν όμορφες εικόνες με γάτες που κανέναν δεν θα πείραζε αν τις μοιραζόταν. Αλλά σε κάθε περίπτωση, θα πρέπει να έχουμε επίγνωση του τι αναδημοσιεύουμε και επίγνωση του τι λέμε γιατί θα μπορούσε να αναδημοσιευθεί.

Αναδημοσίευση ψεμάτων

Αξίζει επίσης να σημειωθεί ότι παρόλο που οι ερευνητές υπέθεσαν ότι τα περισσότερα από αυτά τα tweets εκθέτουν τη προσωπική ζωή, είναι εξίσου πιθανό ότι πολλά από αυτά να είναι κατασκευασμένα (ψέματα). Αν κάποιος μπορεί να πληκτρολογήσει RT και το όνομά σας, να αποκόψει και να επικολλήσει το μήνυμα, δεν υπάρχει κανένας λόγος να πιστέψουμε ότι το μήνυμα που αναρτήθηκε είναι δικό σας. Συχνά οι επεξεργασίες είναι μικρής σημασίας, αλλά δεν υπάρχει τίποτα που να μπορεί να σταματήσει κάποιον από το να δημοσιεύσει κάτι επιζήμιο για τη φήμη κάποιου άλλου. Αν δεν δημοσιεύετε δημόσια προστατεύετε τον εαυτό σας, διότι είναι δύσκολο να γίνει διάψευση για κάποιες αναδημοσιεύσεις, εφ' όσον κανείς δεν μπορεί να ελέγξει τι είναι αυτό που είπατε στη πραγματικότητα και ιδίως όταν πρόκειται για μια δημόσια δημοσίευση που μπορεί να είναι προσβλητική, οι άλλοι θα υποθέσουν ότι την έχετε διαγράψει.

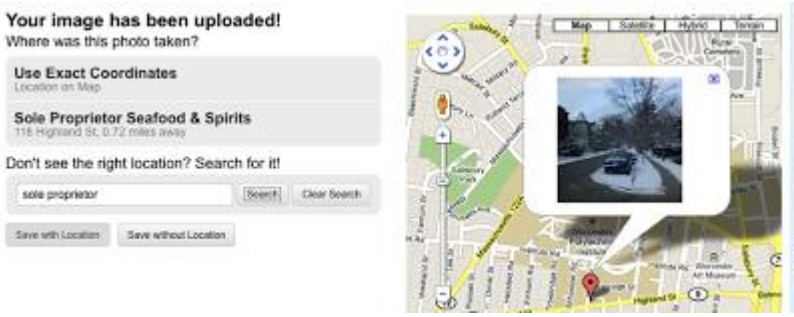
Ενσωματωμένες ρυθμίσεις τοποθεσίας του Twitter

Το twitter έχει κάνει την επιλογή, να είναι δυνατόν να ανακτήσεις αν μία στιγμή συνειδητοποιήσεις ότι έχεις μοιραστεί πάρα πολλές πληροφορίες και θέλεις να διαγράψεις όλα τα δεδομένα των τοποθεσιών που βρέθηκες, για να είσαι ασφαλής:

Πρέπει να είστε πολύ προσεκτικοί σχετικά με τον όγκο των πληροφοριών που μοιράζεστε στο διαδίκτυο. Μπορεί κάποιες πληροφορίες που αναρτήσατε να θέλετε να τις μοιραστείτε, όπως τη θέση σας και μερικές φορές να θέλετε να κρατήσετε τη τοποθεσία που βρίσκεστε κρυφή. Να προσέχετε να μη δημοσιεύετε συντεταγμένες που δεν θέλετε άλλοι να βλέπουν.

Πώς το iPhone σας μπορεί να λέει στον καθένα που ζείτε

Πολλά σύγχρονα smartphones, συμπεριλαμβανομένου του iPhone, διαθέτουν ενσωματωμένο GPS έτσι ώστε να μπορείτε να αποθηκεύετε τα δεδομένα της τοποθεσίας που βρίσκεστε σε κάθε φωτογραφία. Αυτό είναι έξυπνο, όταν πρόκειται για ταξινόμηση φωτογραφιών, αλλά επειδή αυτή η πληροφορία αποθηκεύεται στη φωτογραφία, κάθε εικόνα που μοιράζεστε μπορεί να ενημερώσει κάποιον ακριβώς που είστε (ή που ήσασταν όταν τράβηξατε τη φωτογραφία).



Το ζήτημα εδώ είναι ότι τα χωρικά δεδομένα συχνά καταγράφονται από προεπιλογή. Πολλές φορές μπορεί να είναι επικίνδυνο να μοιράζεστε αυτές τις πληροφορίες. Πολλές υπηρεσίες φωτογραφιών, όπως το Flickr και το Twitpic, σας επιτρέπουν να γενικεύετε τα δεδομένα σας,

έτσι ώστε να εμφανίζεται ότι βρίσκεται σε μια πόλη χωρίς να δείχνει την ακριβή τοποθεσία μέσα στη πόλη. Αλλά μπορεί κανείς να επιλέξει να είναι ορατά.

Φιλοσοφία χρήσης δεδομένων

Από τρίτους: Το Twitter χρησιμοποιεί μια ποικιλία από υπηρεσίες τρίτων για να βοηθήσει την παροχή των Υπηρεσιών μας, όπως φιλοξενώντας διάφορα blogs και wikis, και βοηθώντας να κατανοήσουμε τη χρήση των Υπηρεσιών όπως το Google Analytics. Αυτές οι υπηρεσίες τρίτων μπορούν να συλλέξουν πληροφορίες που αποστέλλονται από το πρόγραμμα περιήγησής σας ως μέρος αίτησης για μια σελίδα του web, όπως τα cookies ή την IP διεύθυνση σας. Οι τρίτοι και οι συνεργάτες τους μπορούν να μοιράζονται πληροφορίες μαζί σας, όπως ένα αναγνωριστικό cookie του προγράμματος περιήγησης ή κρυπτογραφικές hash ενός κοινού αναγνωριστικού λογαριασμού (όπως μια διεύθυνση ηλεκτρονικού ταχυδρομείου), για να σας βοηθήσουν να αξιολογήσετε την ποιότητα της διαφήμισης.

Για παράδειγμα, αυτό επιτρέπει να προβάλλονται διαφημίσεις για πράγματα που μπορεί να έχετε εκδηλώσει ενδιαφέρον. Φυσικά, μπορείτε να απενεργοποιήσετε τις προσαρμοσμένες διαφημίσεις από τις ρυθμίσεις του απορρήτου σας, έτσι ώστε ο λογαριασμός σας να μην αντιστοιχίζεται με τις πληροφορίες που μοιράζονται οι εταίροι διαφημίσεων για την προσαρμογή διαφημίσεων.

Tweets, ακολουθίες, λίστες και άλλες δημόσιες πληροφορίες: Οι υπηρεσίες του twitter σχεδιάστηκαν για να βοηθήσουν τους χρήστες να μοιραζόμαστε πληροφορίες με τον υπόλοιπο κόσμο. Οι περισσότερες από τις πληροφορίες που παρέχουμε στο twitter είναι στοιχεία που θέλουμε να γίνουν δημόσια. Αυτό περιλαμβάνει όχι μόνο τα μηνύματα που δημοσιεύονται ως Tweet αλλά και τα μεταδεδομένα που παρέχονται με τα Tweets, αλλά και οι λίστες που δημιουργείτε, τα άτομα που ακολουθείτε, τα Tweets που έχετε σημειώσει ως αγαπημένα ή αναδημοσιεύετε, και πολλές άλλες πληροφορίες που προκύπτουν από τη χρήση των Υπηρεσιών του Twitter.

Η προεπιλογή του Twitter είναι να κάνει τις πληροφορίες που παρέχετε δημόσιες για όσο χρονικό διάστημα δεν τις διαγράφετε από το Twitter, αλλά γενικά δίνετε η δυνατότητα μέσω ρυθμίσεων να κάνετε τις πληροφορίες σας πιο απόρρητες, αν το επιθυμείτε. Οι δημόσιες

πληροφορίες διαδίδονται ευρέως και στιγμιαία. Για παράδειγμα, οι δημόσιες πληροφορίες του προφίλ και τα δημόσια Tweets μπορούν να αναζητούνται από μηχανές αναζήτησης.

Πρόσθετες πληροφορίες: Μπορείτε να δώσετε πληροφορίες του προφίλ σας για να δημοσιοποιήσει το Twitter, όπως ένα σύντομο βιογραφικό, τη τοποθεσία σας, την ιστοσελίδα σας, ή μια φωτογραφία. Μπορείτε να παρέχετε πληροφορίες για να προσαρμόσετε τον λογαριασμό σας, όπως έναν αριθμό κινητού τηλεφώνου για την παράδοση των μηνυμάτων SMS. Μπορείτε να χρησιμοποιήσετε τα στοιχεία επικοινωνίας σας για να σας αποστέλλονται πληροφορίες σχετικά με τις υπηρεσίες του Twitter.

Μπορείτε να χρησιμοποιήσετε τις ρυθμίσεις του λογαριασμού σας για να διαγραφείτε από τις ειδοποιήσεις του Twitter. Μπορείτε επίσης να διαγραφείτε, ακολουθώντας τις οδηγίες που περιέχονται σε κοινοποίηση ή τις οδηγίες που εμφανίζονται στην ιστοσελίδα σας. Μπορείτε να χρησιμοποιήσετε τα στοιχεία επικοινωνίας σας για να βοηθήσετε τους άλλους να βρουν τον Twitter λογαριασμό σας, συμπεριλαμβανομένων υπηρεσιών τρίτων και εφαρμογές πελατών. Οι ρυθμίσεις απορρήτου σας ορίζουν εάν οι άλλοι μπορούν να σας βρουν με τη διεύθυνση του ηλεκτρονικού σας ταχυδρομείου ή τον αριθμό τηλεφώνου σας. Μπορείτε να επιλέξετε να φορτώσετε το βιβλίο διευθύνσεών σας, έτσι ώστε να μπορέσετε να βρείτε χρήστες του Twitter που γνωρίζετε.

4.4 Αρχιτεκτονικές δικτύων κοινωνικής δικτύωσης

Παρακάτω παρουσιάζονται προτεινόμενες αρχιτεκτονικές δικτύων κοινωνικής δικτύωσης, οι οποίες λαμβάνουν στο σχεδιασμό και την δομή τους την προστασία των προσωπικών δεδομένων.

4.4.1 Αρχιτεκτονική DECENT

Η DECENT[14], μια αρχιτεκτονική για την εφαρμογή ελέγχου πρόσβασης σε ένα αποκεντρωμένο SNS . Εστιάζει στο να παρέχει εμπιστευτικότητα των δεδομένων, ακεραιότητα, διαθεσιμότητα στην παρουσία κακόβουλων κόμβων σε ένα κατανεμημένο περιβάλλον. Η αρχιτεκτονική αυτή είναι επίσης ικανή να προστατεύσει την ιδιωτικότητα των σχέσεων των χρηστών.

Η DECENT είναι βασισμένη σε ένα ευέλικτο αντικειμενοστραφούς σχεδιασμού περιβάλλον (OOD), το οποίο υποστηρίζει τις βασικές λειτουργίες των SNS και αποτυπώνει τις πολύπλοκες και πολλαπλά κύριες αλληλεπιδράσεις που είναι κοινές στα κοινωνικά δίκτυα. Η εμπιστευτικότητα και η ακεραιότητα των δεδομένων προστατεύονται από ένα κρυπτογραφικό μηχανισμό, έτσι ώστε να μπορούν να αποθηκεύονται σε μη αξιόπιστους κόμβους σε ένα κατανεμημένο πίνακα κατακερματισμού (DHT). Οι τυποποιημένοι μηχανισμοί του DHT έχουν επεκταθεί ώστε να διασφαλίζεται η διαθεσιμότητα, παρά τις κακόβουλες προσπάθειες να σβήσουν ή να αλλάξουν τα αποθηκευμένα δεδομένα.

Μεγάλο μέρος της λειτουργικότητας των SNS, μπορεί να περιγραφεί καθώς οι χρήστες δημοσιεύουν περιεχόμενο και τις κοινωνικές επαφές τους, σχολιάζοντας και συμπληρώνοντας το εν λόγω περιεχόμενο. Για την παροχή ενός ευέλικτου, γενικού μοντέλου τέτοιων πράξεων, ορίζουμε έναν περιέκτη αντικειμένων που έχει δύο συνιστώσες: το κύριο περιεχόμενο και μια λίστα με τις παρατηρήσεις / σχόλια, που εκπροσωπήθηκαν ως αναφορές σε άλλα αντικείμενα του περιέκτη. Το κύριο περιεχόμενο μπορεί να πάρει πολλά είδη, όπως μια ενημερωμένη κατάσταση, ένα κοινό σύνδεσμο, μια φωτογραφία ή βίντεο, ή μια συλλογή από αντικείμενα του περιέκτη (π.χ. ένα άλμπουμ με φωτογραφίες).

Το προφίλ ενός χρήστη είναι η ρίζα του αντικειμένου, η οποία περιέχει αναφορές σε άλλα αντικείμενα, όπως στοιχεία επικοινωνίας, τον τοίχο, άλμπουμ φωτογραφίας, κλπ. Ομοίως, άλλα

αντικείμενα μπορεί να συνίστανται από περιεχόμενα και αναφορές σε άλλα αντικείμενα. Για παράδειγμα, ένας τοίχος μπορεί να έχει αναφορές σε μηνύματα της κατάστασης και να δημοσιεύει ένα αντικείμενο κατάστασης που μπορεί να περιέχει αναφορές σε αντικείμενα σχολίων πέραν των δεδομένων της κατάστασης.

Έτσι, το περιεχόμενο του κάθε χρήστη είναι οργανωμένο με ιεραρχικό τρόπο (παρόλα αυτά δεν επιβάλλουμε μια δενδροειδή δομή-ένα αντικείμενο από μόνο του μπορεί να αναφέρεται σε πολλαπλούς "γονείς" αντικείμενα). Με αυτό το βαθμό διακριτικότητας στο σχεδιασμό του αντικειμένου μας, τα δικαιώματα πρόσβασης μπορούν να ανατεθούν συγκεκριμένα για κάθε αντικείμενο και στη συνέχεια να παραπέμπει σε άλλους περιέκτες.

Μέσα σε αυτό το μοντέλο, μπορούμε να σκιαγραφήσουμε μια σειρά από απαιτήσεις ασφάλειας και προστασίας της Ιδιωτικότητας:

- Εμπιστευτικότητα: Η διατήρηση της εμπιστευτικότητας του περιεχομένου των χρηστών είναι η βασική προϋπόθεση για ένα αποκεντρωμένο SNS. Το περιεχόμενο θα πρέπει να είναι προσβάσιμο μόνο από εκείνους που είναι ρητά εξουσιοδοτημένοι από τον ιδιοκτήτη του περιεχομένου. Επιπλέον, οι κόμβοι φιλοξενίας των δεδομένων, δεν είναι εξουσιοδοτημένοι για να διαβάσουν τα δεδομένα.

- Ακεραιότητα: Πρέπει επίσης να διασφαλίσουμε την ακεραιότητα των δεδομένων έτσι ώστε οι χρήστες SNS να είναι βέβαιοι ότι το περιεχόμενο που δημοσιεύτηκε από τους φίλους του είναι αυθεντικό. Αυτή η ιδιότητα είναι σημαντική σε ένα peer-to-peer δίκτυο εφ' όσον οι κόμβοι αποθήκευσης είναι μη αξιόπιστοι και μπορεί να προσπαθήσουν να εκτελέσουν μη εξουσιοδοτημένες ενημερώσεις στα αποθηκευμένα δεδομένα.

- Διαθεσιμότητα: το περιεχόμενο του χρήστη θα πρέπει να παραμείνει διαθέσιμο μέχρι να διαγραφεί οριστικά από τον ιδιοκτήτη του, ακόμη και αν ο ιδιοκτήτης είναι offline, και παρά τις κακόβουλες προσπάθειες να καταστρέψουν τα δεδομένα. Οι αναγνώστες θα πρέπει επίσης να είναι σε θέση να ανακτήσουν την πιο πρόσφατη έκδοση της εμφάνισης του περιεχομένου ενός αντικειμένου και όχι μία παλιά.

- Σαφής Ιδιοκτήτης - προσδιορίζεται έλεγχος πρόσβασης: Πολιτικές έλεγχου όπως ποιος μπορεί να δει, να τροποποιεί, ή να σχολιάζει το περιεχόμενο, ορίζονται από τον ιδιοκτήτη του και δεν μπορεί να αλλάξει, χωρίς την άδεια του.

- Ιδιωτικότητα σχέσεων: οι σχέσεις μεταξύ των χρηστών πρέπει να παραμένουν κρυφές από τρίτους, που ενδέχεται να μην έχουν σχέση με τον ιδιοκτήτη του αντικειμένου και είναι επομένως αναξιόπιστοι κόμβοι αποθήκευσης.

Ωστόσο, η επιτυχία των SNS κατέληξε εις βάρος της Ιδιωτικότητας των χρηστών. Οι χρήστες δεν έχουν τον έλεγχο των δεδομένων τους και εξαρτώνται από τον χειριστή του SNS για την προστασία των ευαίσθητων πληροφοριών τους.

Οι προσδοκίες των χρηστών για τη προστασία των προσωπικών δεδομένων είναι συχνά αντίθετες με τα επιχειρηματικά κίνητρα του χειριστή, και στην πραγματικότητα υπάρχουν αρκετοί πάροχοι που έχουν εντοπιστεί και αποδειχθεί ότι πωλούν τα δεδομένα των χρηστών. Το Facebook, MySpace και πολλές άλλες ιστοσελίδες κοινωνικής δικτύωσης έχουν στείλει δεδομένα σε διαφημιστικές εταιρείες που θα μπορούσαν να χρησιμοποιηθούν για να βρουν ονόματα καταναλωτών και άλλα προσωπικά στοιχεία, παρά τις υποσχέσεις ότι δεν μοιράζονται τις εν λόγω πληροφορίες χωρίς συναίνεση.

Η πρακτική αυτή, που οι περισσότερες από τις εταιρείες υπερασπίζονται και σύμφωνα με αυτή λειτουργούν, είναι να στέλνουν τα ονόματα χρηστών ή τους αριθμούς ταυτότητας, συνδέοντας τα με το προσωπικό προφίλ που προβάλλεται όταν οι χρήστες κάνουν κλικ στις διαφημίσεις. Μετά από ερωτήματα που υποβλήθηκαν από την "The Wall Street Journal" [28], το Facebook και το MySpace προσπαθούν να κάνουν αλλαγές σε αυτό το κομμάτι.

Διαφημιστικές εταιρείες λαμβάνουν πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν αναζητώντας στα προφίλ, τα οποία, ανάλογα με τις πληροφορίες που ο χρήστης έχει δημοσιοποιήσει, περιλαμβάνουν στοιχεία όπως το πραγματικό όνομα ενός ατόμου, την ηλικία, το επάγγελμα και την πατρίδα.

Μέσω του Web, είναι σύνηθες για τους διαφημιστές να λαμβάνουν τη διεύθυνση της σελίδας από την οποία ένας χρήστης κάνει κλικ σε μια διαφήμιση. Συνήθως, δεν λαμβάνουν τίποτα περισσότερο για τον χρήστη από μια ακατανόητη σειρά γραμμάτων και αριθμών χωρίς να μπορούν να δείξουν την προέλευση του ατόμου. Στους δικτυακούς τόπους κοινωνικής δικτύωσης, συνήθως οι διευθύνσεις αυτές περιλαμβάνουν ονόματα χρηστών που θα μπορούσαν να κατευθύνουν διαφημιστές στη σελίδα του προφίλ τους που είναι γεμάτη με προσωπικές

πληροφορίες. Σε ορισμένες περιπτώσεις, τα ονόματα των χρηστών είναι τα πραγματικά ονόματα των ατόμων.

Για τους περισσότερους ιστότοπους κοινωνικής δικτύωσης, τα στοιχεία προσδιορίζουν το προφίλ που προβάλλεται, αλλά όχι κατ' ανάγκη το πρόσωπο που κάνει κλικ στη διαφήμιση ή τη σύνδεση. Το Facebook, όμως, προχώρησε περισσότερο απ' ότι άλλοι ιστότοποι, σε ορισμένες περιπτώσεις σηματοδοτείτε ποιανού το όνομα χρήστη ή ταυτότητας έκανε κλικ στη διαφήμιση, καθώς το όνομα χρήστη ή η ταυτότητα είναι αναγνωριστικό της σελίδας που προβάλλεται. Βλέποντας τι διαφημίσεις παρακολουθεί ένας χρήστης, ο διαφημιστής θα μπορούσε να βγάλει συμπεράσματα για τα ενδιαφέροντα του χρήστη [28].

Επιπλέον, οι πολιτικές των SNS για τη προστασία της ιδιωτικής ζωής είναι συχνά δύσκολο να τις καταλάβει κανείς και οι συνεχείς αλλαγές σε αυτές μεγεθύνει ακόμη περισσότερο το πρόβλημα. Επιπλέον, οι υπάρχουσες κεντρικές αρχιτεκτονικές παρουσιάζουν ένα σημείο αποτυχίας του συστήματος. Κάθε έλλειψη σε αυτά τα συστήματα ακούσια ή μη, μπορεί να χρησιμοποιηθεί από ένα κακόβουλο αντίπαλο και να αποκτήσει χωρίς αποκρυπτογράφηση ευαίσθητα δεδομένα χρηστών.

Αυτή η έλλειψη Ιδιωτικότητας των χρηστών που έχουν αναπτύξει τα SNS, έχουν ωθήσει την έρευνα στο σχεδιασμό μηχανισμών για την διαφύλαξη της ιδιωτικής ζωής στη κοινωνική δικτύωση.

Αποκεντρωμένες αρχιτεκτονικές μπορούν να αντιμετωπίσουν αυτό το ζήτημα. Ακόμη παρουσιάζεται μια νέα σειρά προκλήσεων, όπως εκτός από την εμπιστευτικότητα και την ακεραιότητα, η προστασία που η κρυπτογραφία μπορεί να προσφέρει, είναι απαραίτητο να διασφαλιστεί, η διαθεσιμότητα και η αποτελεσματική πρόσβαση σε δεδομένα που είναι υποχρεωτικό να υποστηρίζουν κοινές SNS λειτουργίες, όπως ένα «News feed».

Η κρυπτογράφηση αποθηκευμένου περιεχομένου μπορεί να παρέχει ισχυρές εγγυήσεις εμπιστευτικότητας, αλλά χρειαζόμαστε online ταυτοποίηση των ενημερώσεων και των σχολίων για να εξασφαλιστεί η διαθεσιμότητα των δεδομένων. Επιπλέον, αποδίδουν με βάση συστημάτων κρυπτογράφησης που παρέχουν εξαιρετικά ευέλικτες πολιτικές που είναι υπολογιστικά ακριβές και συμβάλλουν σημαντικά στην απόδοση του συστήματος. Συμφωνούμε ότι για να έχουμε αποτελεσματική υποστήριξη στη σύνθετη λειτουργικότητα ενός SNS, ένας συνδυασμός μεθόδων πρέπει να χρησιμοποιηθεί.

Δείξαμε πως η εμπιστευτικότητα και η ακεραιότητα των δεδομένων μπορεί να προστατευτεί από ένα μηχανισμό κρυπτογράφησης, έτσι ώστε να μπορούν να αποθηκεύονται σε μη αξιόπιστους κόμβους ενός DHT (κατανεμημένου πίνακα κατακερματισμού). Ωστόσο, ο σχεδιασμός πάσχει στην επίδοση, σε ζητήματα που προκύπτουν λόγω της ανάκτησης και της αποκρυπτογράφησης εκατοντάδων μικρών αντικειμένων που ανήκουν σε φίλους, που απαιτούνται για την προβολή στους τοίχους τους ή για την προβολή του δικού τους News feed.

4.4.2 Cachet, μια αποκεντρωμένη αρχιτεκτονική

Η Cachet [21], μια αποκεντρωμένη αρχιτεκτονική για κοινωνικά δίκτυα που παρέχει ισχυρή ασφάλεια και προστασία της Ιδιωτικότητας, ενώ υποστηρίζει αποτελεσματικά τη κεντρική λειτουργικότητα των SNS. Το κέντρο της Cachet είναι ένα υβριδικό δομημένο-αδόμητο επίστρωμα στο οποίο ένας συμβατικός πίνακας διανομής κατακερματισμού αυξάνεται με social links μεταξύ των χρηστών. Χρησιμοποιεί τον πίνακα διανομής κατακερματισμού ως στρώμα αποθήκευσης , αλλά προσθέτει έναν αλγόριθμο (gossip-based social caching algorithm) και αυξάνεται σημαντικά η απόδοση.

Νέες ενημερώσεις μεταδίδονται άμεσα στις κοινωνικές επαφές που βρίσκονται online. Όταν ένας online χρήστης επιστρέφει πίσω online, ένα πρωτόκολλο χρησιμοποιείται για να εντοπίζει επαφές που βρίσκονται σε απευθείας σύνδεση και αναζητά άμεσα ενημερώσεις.

Επιπλέον, αυτές οι επαφές χρησιμοποιούνται για την ανάκτηση προσωρινά αποθηκευμένων ενημερώσεων από αμοιβαίες (ή κοινές) επαφές, που είναι σε απευθείας σύνδεση καθώς η ταχύτητα οφείλεται στην ανακάλυψη άλλων online επαφών. Ο DHT (κατανεμημένος πίνακας κατακερματισμού) χρησιμοποιείται για την ανάκτηση των ενημερώσεων που δεν μπορούν να αποθηκευτούν προσωρινά, διασφαλίζοντας υψηλή διαθεσιμότητα των δεδομένων.

Όπως αναφέρθηκε προηγουμένως, ενώ αρκετά έργα έχουν προταθεί για την ενίσχυση της προστασία της ιδιωτικής ζωής των SNS, η Cachet είναι η πρώτη που έχει ολοκληρωμένο σχεδιασμό για SNS και συνδυάζει την αποκέντρωση, τη κρυπτογράφηση βασισμένη στα

χαρακτηριστικά και τη χρήση της κρυφής μνήμης για την παροχή υψηλής διαθεσιμότητας, λίγες λανθάνουσες καταστάσεις και ευέλικτες πολιτικές για την προστασία των δεδομένων.

Τα δεδομένα στην Cachet αποθηκεύονται σε περιέκτες αντικειμένων που περιλαμβάνουν περιεχόμενο, όπως ενημερώσεις καταστάσεων και φωτογραφίες, καθώς και αναφορές σε άλλους περιέκτες. Εξουσιοδοτεί επαφές που μπορούν να προσθέσουν σχόλια ή άλλα σχόλια σε περιέκτες. Ένας περιέκτης προστατεύεται από μια δομή κρυπτογράφησης που διασφαλίζει την εμπιστευτικότητα και την ακεραιότητα, ενώ υποστηρίζει πολλαπλές-κύριες αλληλεπιδράσεις χωρίς να αποκαλύψει τις πολιτικές ή τις σχέσεις του χρήστη με τους κόμβους αποθήκευσης.

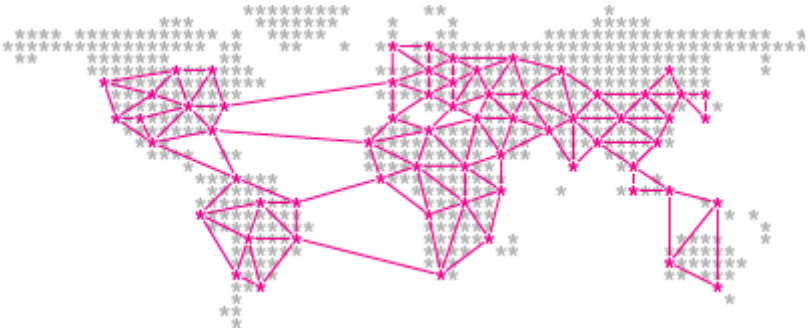
Η δομή περιλαμβάνει δυνατότητες κρυπτογράφησης που χρησιμοποιούνται από τους κόμβους αποθήκευσης για τον έλεγχο ταυτότητας, ενημερωμένα αιτήματα και κρυπτογράφηση βασισμένη στα χαρακτηριστικά που χρησιμοποιούνται για την παροχή ευέλικτων και λεπτών πολιτικών πρόσβασης.

Για να μειώσουν το κόστος της προσωρινής αποθήκευσης οι περιέκτες αποθηκεύονται σε μορφή αποκρυπτογράφησης και χρησιμοποιούνται από κοινού με άλλες επαφές αφού επαληθευθεί ότι πληρούν την αντίστοιχη πολιτική πρόσβασης, ως εκ τούτου, οι περιέκτες πρέπει να αποκρυπτογραφηθούν άμεσα μόνο όταν είναι απαραίτητο από τον DHT. Οι κόμβοι αποθήκευσης είναι αξιόπιστοι μόνο για να παρέχουν διαθεσιμότητα των δεδομένων με τη χρήση της αντιγραφής και για να υπερασπιστεί σε περίπτωση που οι κόμβο έχουν κάποιες αποτυχίες ή εσκεμμένα κακή συμπεριφορά.

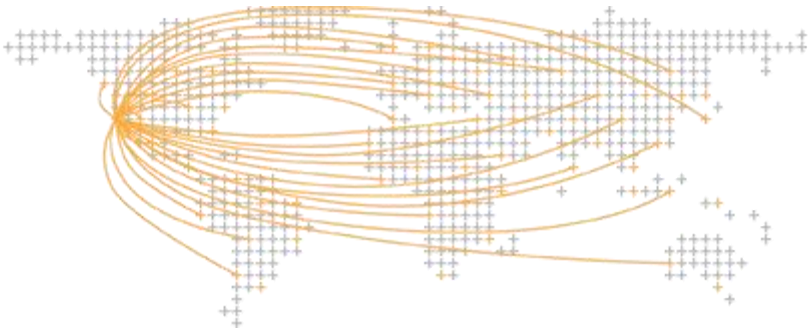
Αυτή η αρχιτεκτονική μας δείχνει πώς ένα προσεκτικός συνδυασμός πολλών κατανεμημένων συστημάτων, κρυπτογράφησης και τεχνικών μπορούν να χρησιμοποιηθούν για να παρέχουν μια συγκλονιστική επιλογή για τη διαφύλαξη της ιδιωτικής ζωής στα SNS.

4.4.3 Diaspora*

Το Diaspora* [39] είναι ένα πραγματικό δίκτυο κοινωνικής δικτύωσης, χωρίς κεντρική βάση. Υπάρχουν εξυπηρετητές (κόμβοι) σε όλο τον κόσμο, που ο καθένας περιέχει τα δεδομένα των χρηστών που έχουν επιλέξει να εγγραφούν σε αυτόν. Οι κόμβοι αυτοί επικοινωνούν μεταξύ τους αρμονικά, έτσι ώστε να μπορεί να εγγραφεί κανείς σε οποιοδήποτε κόμβο και να επικοινωνεί ελεύθερα με τις επαφές του, όπου κι αν βρίσκεται στο δίκτυο.



Τα περισσότερα κοινωνικά δίκτυα τρέχουν πάνω σε κεντρικούς εξυπηρετητές που ανήκουν και διοικούνται από μια εταιρεία και αποθηκεύουν όλα τα προσωπικά δεδομένα των χρηστών τους. Αυτές οι πληροφορίες μπορεί να χαθούν ή να υποκλαπούν, και όπως κάθε σύστημα με μια κεντρική βάση, κάθε πρόβλημα στους κεντρικούς εξυπηρετητές μπορεί να κάνει το σύνολο του δικτύου να τρέχει πολύ αργά ή και καθόλου. Επίσης, είναι πιο εύκολο για τις κυβερνήσεις να “ακούσουν” οποιαδήποτε ανταλλαγή πληροφοριών.



Το Diaspora* δεν χρησιμοποιεί τα δεδομένα για κανέναν άλλο σκοπό εκτός από το να επιτρέπει να συνδεθεί κανείς και να τα μοιραστεί με άλλους.

Επιλέγει ο καθένας που θα αποθηκεύονται τα δεδομένα του, με την επιλογή ενός κόμβου τον οποίο επιλέγει ο ίδιος. Αν θέλει κανείς να είναι πραγματικά ασφαλής, μπορεί να δημιουργήσει και να φιλοξενήσει τον δικό του κόμβο σε εξυπηρετητές που ελέγχει, ώστε να μην μπορεί κανείς να πάρει τα προσωπικά του δεδομένα. Ένα σημαντικό χαρακτηριστικό του Diaspora* που ονομάζεται πτυχές, επιτρέπει το διαμοιρασμό πληροφορίας μόνο με εκείνους τους ανθρώπους που θέλει ο χρήστης.

Κεφάλαιο 5
Χρήση PETs στα SNS

Στο κεφαλαίο αυτό θα δείξουμε το βαθμό διείσδυσης των τεχνολογιών προστασίας της Ιδιωτικότητας στον τομέα των δικτύων κοινωνικής δικτύωσης, σύμφωνα με την τρέχουσα διεθνή βιβλιογραφία, αλλά και τους παράγοντες που αντιτίθενται στην διαδικασία αυτή. Θα αναφερθούμε σε παράγοντες που οδηγούν στη χαμηλή αξιοποίηση τεχνολογιών ενίσχυσης της Ιδιωτικότητας σε περιβάλλοντα κοινωνικών δικτύων.

5.1 Παράγοντες που επηρεάζουν την υιοθέτηση των PETs από τους χρήστες των SNS

Μελετώντας τη πρόσφατη βιβλιογραφία, σταθήκαμε στη μελέτη των Βέμου και Καρύδα [31], που αναλύουν τους λόγους για τους οποίους, ενώ τα δίκτυα κοινωνικής δικτύωσης αποκτούν ολοένα και περισσότερα ενεργά μέλη και συνεχώς παρουσιάζονται κενά ασφαλείας σε ότι αφορά την προστασία των προσωπικών δεδομένων , δεν παρουσιάζεται αντίστοιχη αύξηση της υιοθέτησης τεχνολογιών προστασίας της Ιδιωτικότητας.

Ευαισθητοποίηση για την Προστασία Προσωπικών Δεδομένων

Έχει προταθεί, ότι πολλοί χρήστες SNS αγνοούν την ύπαρξη ορισμένων PETs [11]. Επιπλέον, υπάρχει περίπτωση οι χρήστες να μη γνωρίζουν για τη προστασία της ιδιωτικής ζωής, ούτε για τις απειλητικές πτυχές των υπηρεσιών που χρησιμοποιούν, όπως, για παράδειγμα, τους κινδύνους διαρροής προσωπικών δεδομένων από εφαρμογές τρίτων [32]. Ως εκ τούτου, δεν μπορούν να επωφεληθούν από τα PETs, εφ' όσον αυτές αποσκοπούν στον περιορισμό της πρόσβασης εφαρμογών τρίτων σε προσωπικές πληροφορίες.

Συμπερασματικά, η γνώση των εργαλείων προστασίας της ιδιωτικής ζωής αποτελεί βασική προϋπόθεση για τη χρήση τους, η συνειδητοποίηση συνδέεται πολύ λίγο με την ανάπτυξή τους. Είναι επομένως, σημαντικό, να συμπεριλάβουμε και άλλους , καθώς και τεχνικούς παράγοντες, προκειμένου να αποκτήσουμε μια βαθύτερη κατανόηση του προβλήματος.

Απαιτήσεις για Ειδικές γνώσεις τεχνολογιών πληροφορικής

Η έλλειψη τεχνικών δεξιοτήτων και ο χρόνος που απαιτείται για να μάθουν οι χρήστες να χρησιμοποιούν μια τεχνολογία, έχουν επίσης εντοπιστεί ως πιθανή αναστολείς για τη χρήση των

PETs [18]. Όπως αναφέρεται στο άρθρο του Yao (2011) [34], πολλές online στρατηγικές για την προστασία της ιδιωτικής ζωής απαιτούν τεχνικές δεξιότητες πέρα από αυτές ενός μέσου χρήστη.

Πολυπλοκότητα και Διαφορετικότητα

Η ανάγκη για προστασία της ιδιωτικής ζωής, συμπεριλαμβανομένης της υιοθέτησης των PETs, πηγάζει από μια σειρά πολλών και διαφόρων κινδύνων, που απορρέουν από τις διάφορες πτυχές χρήσης της κοινωνικής δικτύωσης, π.χ. ανάρτηση φωτογραφιών, συνομιλίες, δημοσιεύσεις. Όλο αυτό έχει ως αποτέλεσμα να εφαρμόζονται διάφορες πρακτικές για την προστασία της ιδιωτικής ζωής του χρήστη. Μερικές στοχεύουν στην ευαισθητοποίηση και κάποιες στοχεύουν στην απόκρυψη πληροφοριών.

Αυτό δίνει τη δυνατότητα στο χρήστη, να αξιολογήσει πολλά και ποικίλα εργαλεία και τεχνολογίες, προκειμένου να επιλέξει ποιο από αυτά θα χρησιμοποιήσει. Πρόκειται για μια διαδικασία που απαιτεί χρόνο, προσπάθεια και γνώση. Εκτός από την ποικιλία των PETs, οι χρήστες συναντούν πολύπλοκες και άχρηστες διεπαφές [29] που κάνουν τα εργαλεία αυτά πιο δύσκολο να ρυθμιστούν [17], αυξάνοντας έτσι τη δυσκολία της υιοθέτησης των PETs.

Άμεσο και έμμεσο κόστος

Όπως και άλλα προϊόντα λογισμικού, η χρήση των PETs μπορεί να επιφέρει ένα άμεσο κόστος για την απόκτηση του, καθώς και δαπάνη χρόνου για μάθηση [08] περιορισμένης λειτουργικότητας και χρηστικότητας θέματα, όπως πόσο ομαλή είναι η ταυτοποίηση ιστοσελίδων τρίτων κ.λπ. Οι περισσότεροι χρήστες αναφέρουν ότι δεν είναι πάντα πρόθυμοι να πληρώσουν για την απόκτηση ενός τέτοιου εργαλείου, παρά το γεγονός ότι αφορά την προστασία της ιδιωτικής τους ζωής.

Επιπλέον, στους χρήστες των υπηρεσιών κοινωνικής δικτύωσης αρέσει να βιώνουν καταστάσεις άμεσα. Δεν είναι πρόθυμοι να βιώσουν μια εμπειρία με καθυστέρηση, δηλαδή να πράξουν κάτι που ίσως τους δώσει ικανοποίηση στο μέλλον, ούτε να αλλάξουν τις συνήθειες τους αλληλεπιδρώντας με μια e-υπηρεσία ή προεξοφλώντας τη χρηστικότητα, λόγω χρήσης των PETs [01].

Θέματα αποτελεσματικότητας των PETs

Η ευαισθητοποίηση των χρηστών σχετικά με τα οφέλη που προκύπτουν από τη διατήρηση της ιδιωτικής ζωής τους είναι επίσης ένας κρίσιμος παράγοντας σε σχέση με την απόφασή τους να χρησιμοποιούν εφαρμογές για τη προστασία της Ιδιωτικότητας. Υπάρχουν χρήστες που αναφέρουν ότι δεν πιστεύουν στην αποτελεσματικότητα των PETS [12]. Αυτό μπορεί να οφείλεται, στον τρόπο με τον οποίο τα PETs επικοινωνούν ή μάλλον αποτυγχάνουν να το κάνουν, στα αποτελέσματά τους και τον τρόπο που δίνουν ανατροφοδότηση για τις ενέργειες που έχουν πραγματοποιήσει για τη προστασία του χρήστη [23], ή στον τρόπο που η προστασία της ιδιωτικής ζωής σχετίζεται με τους κινδύνους που παρουσιάζονται από την τεχνολογία που χρησιμοποιείται [15].

Απαιτήσεις Προστασίας Προσωπικών Δεδομένων

Οι περισσότερες τεχνολογίες προώθησης της Ιδιωτικότητας πληρούν συγκεκριμένες απαιτήσεις προστασίας της ιδιωτικής ζωής. Ενώ η προστασία της ιδιωτικής ζωής συνεπάγεται γενικά την προστασία των προσωπικών πληροφοριών από μη εξουσιοδοτημένη συλλογή πληροφοριών, επεξεργασία και διάδοση, ενημερώνοντας τους χρήστες και παρέχοντάς τους τον έλεγχο των προσωπικών τους δεδομένων [20,23], κάθε εργαλείο προστασίας της ιδιωτικής ζωής συνήθως πληροί ένα μόνο μικρό μέρος αυτών των απαιτήσεων.

Ο ρόλος της ίδιας της πλατφόρμας SNS

Μερικές τεχνολογίες ενίσχυσης της Ιδιωτικότητας, πρέπει να υποστηρίζονται από τον πάροχο των υπηρεσιών κοινωνικής δικτύωσης, ώστε οι χρήστες να μπορούν να τις χρησιμοποιούν. Ωστόσο, οι πάροχοι δεν είναι πάντα πρόθυμοι να υποστηρίξουν PETs αν δεν είναι υποχρεωμένοι. Καθώς δεν υπάρχουν ενδείξεις ότι θα αποκτήσουν ανταγωνιστικό πλεονέκτημα με τη θέσπιση χρήσης τεχνολογιών ενίσχυσης της Ιδιωτικότητας [09] και την ίδια στιγμή, θα πρέπει να σταματήσουν την συλλογή προσωπικών πληροφοριών, θα πρέπει να πληρώσουν χρήματα για την απόκτησης μιας τέτοιας τεχνολογίας, και θα πρέπει να κάνουν τεχνικές αλλαγές στην υποδομή τους[10].

Υπευθυνότητα Παρανοήσεων

Όταν πρόκειται για την προστασία της ιδιωτικής ζωής, πολλοί χρήστες έχουν την πεποίθηση ότι οι πάροχοι και η κυβέρνηση εφαρμόζουν τα αναγκαία μέτρα για την εξασφάλισή της. Δεν γνωρίζουν ότι η προστασία της ιδιωτικής ζωής είναι εν μέρει ευθύνη του καθενός.

Πολύπλοκες πολιτικές απορρήτου δημοσιεύονται στα περισσότερα SNS, δίνουμε αυτό το χαρακτηρισμό διότι πολλοί χρήστες παρερμηνεύουν την εμφάνισή τους, ως ενεργοποίηση της προστασίας της ιδιωτικής ζωής. Από την άλλη πλευρά, τα SNS είναι δύσκολο να συμμορφωθούν με τους κανονισμούς προστασίας προσωπικών δεδομένων, λόγω της έλλειψης μηχανισμών λογοδοσίας [04].

5.2 Ενσωμάτωση της έννοιας της προστασίας της Ιδιωτικότητας στα SNS

Στη μελέτη των Βέμου και Καρύδα [30], αναφέρεται ότι η ενσωμάτωση των μηχανισμών προστασίας της ιδιωτικής ζωής έχει από καιρό δηλωθεί ως πρόβλημα στη βιβλιογραφία, με διάφορες προσεγγίσεις να προτείνονται, ωστόσο, εξακολουθεί να μην υπάρχει σαφής μεθοδολογία ή πλαίσιο για τη προστασία της ιδιωτικής ζωής. Τον τελευταίο καιρό, η έννοια Προστασίας Προσωπικών Δεδομένων-από το Σχεδιασμό τους [05], με στόχο την ενίσχυση της προστασίας της ιδιωτικής ζωής σε συστήματα πληροφορικής από την αρχή της λειτουργίας τους ή ακόμη και από το σχεδιασμό τους, έχει αναδειχθεί ως μια επιτακτική ανάγκη για την προστασία της ιδιωτικής ζωής.

Οι αρχές αυτές, αν και είναι πολύ γενικές, θα μπορούσαν να υιοθετηθούν από τις πλατφόρμες SNS, για την προστασία της ιδιωτικής ζωής των χρηστών και να ανακτήσουν τη χαμένη εμπιστοσύνη των χρηστών.

Συμπερασματικά, όσο σημαντική και αν είναι η προστασία της ιδιωτικής ζωής, οι τρέχουσες στρατηγικές αδυνατούν να παρέχουν στους σχεδιαστές σαφή καθοδήγηση σχετικά με

συγκεκριμένες πρακτικές προστασίας προσωπικών δεδομένων και εργαλεία για την εφαρμογή τους, ιδίως στο πλαίσιο των υπηρεσιών κοινωνικής δικτύωσης. Παρακάτω, αναλύονται στρατηγικές Προστασίας Προσωπικών Δεδομένων, από το Σχεδιασμό τους και απορρέουν συγκεκριμένες απαιτήσεις προστασίας της ιδιωτικής ζωής.

Απαιτήσεις απορρήτου για SNS

Δίνεται ιδιαίτερη προσοχή στην χρηστικότητα και την απόδοση των ενσωματωμένων πρακτικών, διότι η εφαρμογή τεχνολογιών ενίσχυσης της ιδιωτικής ζωής (PET), ακόμη και στην έννοια των ενσωματωμένων πρακτικών, δεν μπορεί πάντα να είναι αποδεκτή από τους χρήστες λόγω των ζητημάτων απόδοσης. Για παράδειγμα, η κρυπτογράφηση προσωπικών πληροφοριών, κάθε φίλος που έχει δικαίωμα θα καθυστερεί να λάβει τις πληροφορίες. Αυτός ο τρόπος λειτουργία καθυστερεί ακόμη περισσότερο όταν οι λίστες των παραληπτών είναι μεγάλες.

Επίσης, η δημιουργία μιας πολύπλοκης διαδικασίας δημοσιευμένων πληροφοριών, π.χ. να χρειάζονται πολλά βήματα για να καθορίσεις το κοινό του δημοσιεύματος, μπορεί να αποθαρρύνει τους χρήστες από τη χρήση της SNS πλατφόρμας. Η ευχρηστία των ρυθμίσεων απορρήτου προστίθενται στην έννοια αυτή. Αν θεωρήσουμε ότι οι SNS πλατφόρμες προσφέρουν ένα ευρύ φάσμα ρυθμίσεων απορρήτου, οι χρήστες δεν επωφελούνται από αυτές [19], λόγω της μη προφανούς θέσης αυτών των ρυθμίσεων στο περιβάλλον κοινωνικής δικτύωσης.

Επίσης, ο χρόνος που χρειάζεται ένας χρήστης να ξοδέψει για να διαχειριστεί τις ρυθμίσεις του απορρήτου του, μπορεί να είναι ένας παράγοντας που εμποδίζει την ανάπτυξης τους. Για τους λόγους αυτούς, οι πλατφόρμες κοινωνικής δικτύωσης θα πρέπει να οργανώσουν τις ρυθμίσεις απορρήτου σε μία εύκολα προσβάσιμη τεχνολογία που να εξηγεί τι ρύθμιση πρέπει να κάνουμε για να αποφύγουμε συγκεκριμένους κινδύνους ή να εμφανίζουν οδηγό χρήσης κατά τη διαδικασία των ρυθμίσεων. Το πρώτο σύνολο απαιτήσεων που εντοπίστηκε αναφέρεται στην ελαχιστοποίηση του ποσού των προσωπικών πληροφοριών που επεξεργάζονται οι SNS πλατφόρμες.

Πρακτικές αυτής της κατηγορίας εστιάζονται στη διαδικασία συλλογής πληροφοριών, απαιτούν τη συλλογή ενός περιορισμένου συνόλου πληροφοριών ή την επιλογή του χρήστη να αρνηθεί τη

συλλογή διαφόρων τύπων πληροφοριών. Οι SNS πλατφόρμες μπορούν να ενισχύσουν την προστασία της ιδιωτικής ζωής, επιτρέποντας τη χρήση ψευδωνύμων και ζητώντας ελάχιστες πληροφορίες κατά τη διάρκεια της εγγραφής, αποφεύγοντας δεδομένα που θα μπορούσαν να οδηγήσουν στην ταυτοποίηση του χρήστη, όπως η ημερομηνία γέννησης. Στο χρήστη θα πρέπει να παρέχεται η λειτουργία ευαισθητοποίησης για τον έλεγχο της αναγνωρισιμότητας του. Στην περίπτωση τρίτων εφαρμογών που ζητούν πρόσβαση σε προσωπικές πληροφορίες των χρηστών, η πλατφόρμα κοινωνικής δικτύωσης μπορεί να εφαρμόσει ελέγχους για να διασφαλίσει ότι ζητούν τις ελάχιστες πληροφορίες, αντί να τις ζητήσουν ως προαπαιτούμενο για την εγκατάσταση.

Το δεύτερο σύνολο απαιτήσεων σχετίζεται με απόκρυψη προσωπικών πληροφοριών. Εάν στο χρήστη δοθεί η δυνατότητα να εμποδίσει την πρόσβαση σε ορισμένα είδη πληροφοριών που δημοσιεύονται και μπορεί να δηλώνει ρητά αν το προφίλ του θα είναι δημόσιο ή ανακτήσιμο μέσα από τις μηχανές αναζήτησης, έξω από την πλατφόρμα κοινωνικής δικτύωσης, αυτό θα μπορούσε να συμβάλει στην προστασία της ιδιωτικής ζωής έναντι σε ανεπιθύμητο κοινό. Από άποψη λειτουργίας ελέγχου πρόσβασης, η πλατφόρμα μπορεί να παρέχει τη δυνατότητα να εφαρμόζονται διαφορετικοί έλεγχοι πρόσβασης σε κάθε κομμάτι πληροφοριών που δημοσιεύεται, π.χ. σε διάφορα φωτογραφικά άλμπουμ ή να ορίσετε συγκεκριμένες ομάδες χρηστών, το οποίο θα χορηγήσει πρόσβαση σε συγκεκριμένα τμήματα του προφίλ.

Οι SNS πλατφόρμες μπορούν να ενισχύσουν τη διαφάνεια και την προβολή, ενημερώνοντας τους χρήστες όταν τα προσωπικά τους στοιχεία συλλέγονται ή έχουν προσπελαστεί και προσφέροντας σχετικές εκθέσεις, εφόσον ζητηθούν. Πιο συγκεκριμένα, στους χρήστες μπορεί να παρέχεται μια λειτουργία για να ελέγχουν ποιες από τις πληροφορίες τους είναι διαθέσιμες σε άλλους φορείς .

Οι χρήστες θα πρέπει επίσης να έχουν τον έλεγχο των πληροφοριών τους, ακόμη να είναι σε θέση να ζητήσουν με αίτηση την πλήρη διαγραφή τους.

Οι SNS πλατφόρμες μπορούν να παρέχουν λειτουργίες αναφοράς εύκολης πρόσβασης, για να αναφέρουν στους χρήστες καταχρηστική συμπεριφορά ή κλοπή ταυτότητας. Επίσης, για την εφαρμογή της στρατηγικής απόκρυψης, τα SNS μπορούν να λάβουν μέτρα για τον έλεγχο πρόσβασης και να παραχωρήσουν στους χρήστες αποκλειστικό έλεγχο πρόσβασης στις πληροφορίες τους, αυτό σημαίνει, ότι οι ρυθμίσεις απορρήτου των φίλων θα μας προστατέψουν από ανεπιθύμητη δημοσίευση των πληροφοριών μας.

Αυτό ισχύει επίσης και για την πρόσβαση στις πληροφορίες μας, από εφαρμογές τρίτων κατασκευαστών. Επιπλέον, δεδομένου ότι οι πληροφορίες περιεχομένου είναι τόσο σημαντικές όσο και τα προσωπικά δεδομένα, η πλατφόρμα κοινωνικής δικτύωσης μπορεί να ασπαστεί την τεχνολογία για να επισυνάψει ενιαίες πληροφορίες περιεχομένου και να ενημερώνει σχετικά με την αποδεκτή χρήση (π.χ. τεχνολογία σήμανσης της προστασίας της ιδιωτικής ζωής). Επιπλέον, οι SNS πλατφόρμες μπορούν να απενεργοποιήσουν την αυτοματοποιημένη εξαγωγή πληροφοριών για την προστασία των προφίλ των χρηστών από τρίτους.

Κεφάλαιο 6
Συμπεράσματα και περαιτέρω έρευνα

Στο κεφάλαιο αυτό επιχειρείται η εξαγωγή συμπερασμάτων από τη βιβλιογραφική έρευνα που διεξήχθη, για τη σχέση των PETs και SNS. Ενώ υπάρχει ανάγκη για προστασία της Ιδιωτικότητας στα μέσα κοινωνικής δικτύωσης και οι χρήστες γνωρίζουν διάφορα PETs, παρ' όλα αυτά η χρήση τους είναι εξαιρετικά χαμηλή.

6.1 Συμπεράσματα από τη βιβλιογραφία

Η ανάλυσή μας έδειξε ότι η σημασία της ευαισθητοποίησης έχει μάλλον υπερεκτιμηθεί, δεδομένου ότι πολλοί χρήστες έχουν γνώση των διαφόρων τεχνολογιών ενίσχυσης της Ιδιωτικότητας αλλά εξακολουθούν να μην τις χρησιμοποιούν. Το κόστος, τόσο άμεσα όσο και

έμμεσα, συμβάλλει επίσης στη χαμηλή υιοθέτηση τεχνολογιών ενίσχυσης της ιδιωτικότητας, παίζει όμως σημαντικό ρόλο και η πληθώρα των διαφορετικών και πολλών εργαλείων και εφαρμογών που πρέπει να εξεταστούν. Ακόμη, το ζήτημα της πολυπλοκότητας και της χρηστικότητας αποτελούν σημαντικούς και καθοριστικούς παράγοντες για την ανάπτυξη των τεχνολογιών ενίσχυσης της Ιδιωτικότητας. Σημαντικό είναι και το γεγονός ότι οι χρήστες έχουν την τάση να υποτιμούν την αποτελεσματικότητά τους, λόγω του ότι δεν μπορούν να δουν τα αποτελέσματά τους άμεσα.

Τα αποτελέσματα της βιβλιογραφίας δείχνουν, ότι οι ερευνητές ασχολούνται με τις πληροφορίες της ιδιωτικής ζωής σε επίπεδο εξήγησης, μετά σε επίπεδο ανάλυσης και τέλος σε επίπεδο σχεδιασμού και δράσης. Ως εκ τούτου, η έρευνα θα πρέπει να επικεντρωθεί περισσότερο στο σχεδιασμό και στη δράση με έμφαση τη δημιουργία πραγματικά εφαρμόσιμων εργαλείων για την προστασία των πληροφοριών της ιδιωτικής ζωής.

Συγκεκριμένα, διάφορα επίπεδα ανάλυσης [03], συμβουλεύουν τους ερευνητές να θεωρήσουν ότι πρέπει να σχεδιαστούν και να κυκλοφορήσουν, εύκολα στη χρήση εργαλεία και τεχνολογίες προστασίας προσωπικών πληροφοριών για τον καθένα, για ομάδες, για οργανισμούς και για όλη την κοινωνία.

Αναλύοντας σε βάθος τις πλατφόρμες κοινωνικής δικτύωσης, για να προσδιορίσουμε ενσωματωμένες πρακτικές προστασίας της ιδιωτικής ζωής καταλήγουμε ότι τα SNS έχουν υιοθετήσει κάποιες πρακτικές, οι οποίες πληρούν μόνο μερικές από τις απαιτήσεις Ιδιωτικότητας. Οι SNS πλατφόρμες έχουν κάνει βήματα προόδου προς την απόκρυψη στοιχείων των χρηστών και τον έλεγχο των πληροφοριών τους από τους ίδιους τους χρήστες.

Ωστόσο, οι πλατφόρμες για να προσφέρουν προστασία της ιδιωτικής ζωής, μπορούν επιπλέον να απλοποιήσουν τις ρυθμίσεις απορρήτου και να αποτρέψουν μεταβατικούς ελέγχους πρόσβασης, οι οποίοι μπορεί να οδηγήσουν σε κανόνες πρόσβασης που έρχονται σε αντίθεση με τις ρυθμίσεις των χρηστών. Ειδικά όσον αφορά την φιλικότητα προς τον χρήστη, η υπάρχουσα βιβλιογραφία δείχνει ότι οι ρυθμίσεις απορρήτου στις πλατφόρμες κοινωνικής δικτύωσης πρέπει να αναμορφωθούν ώστε να αντανακλούν επαρκώς τις αρχές που παρουσιάζονται στη πολιτική προστασίας προσωπικών δεδομένων των SNS [02].

Συμπερασματικά, αν και οι πλατφόρμες κοινωνικής δικτύωσης φαίνεται να γνωρίζουν την ανάγκη των χρηστών για προστασία της ιδιωτικής ζωής, οι περισσότερες από αυτές

εξακολουθούν να μην έχουν ασπαστεί τη μη εκμετάλλευση των προσωπικών δεδομένων και επιτρέπουν δευτερεύουσες χρήσεις των προσωπικών πληροφοριών.

6.2 Προτάσεις για μελλοντική έρευνα

Η εισαγωγή των κοινωνικών μέσων στη ζωή μας είναι γεγονός, είναι ένας τομέας που πρέπει να διερευνηθεί σε βάθος, διότι νέες δυνατότητες ενσωματώνονται καθημερινά αλλά και περισσότερα καινούργια μέσα κοινωνικής δικτύωσης έρχονται στο προσκήνιο. Τα ενεργά μέλη αυξάνονται μέρα με τη μέρα, κυρίως με τη ραγδαία ανάπτυξη φθηνών φορητών συσκευών και έχουν ήδη κάνει την εμφάνισή τους στην εκπαίδευση, όπου πρέπει να αξιοποιηθούν σωστά και να παρέχουν ασφάλεια και προστασία προσωπικών δεδομένων στους μικρούς χρήστες.

Υπάρχει μια ποικιλία από εργαλεία και τεχνολογίες ενίσχυσης της Ιδιωτικότητας που μπορούν να χρησιμοποιηθούν και είναι πολλοί οι χρήστες που έχουν γνώση αυτών. Θα μπορούσαν να διερευνηθούν σε βάθος τόσο οι τεχνολογίες και τα εργαλεία που παρουσιάστηκαν στη παρούσα μεταπτυχιακή διατριβή, αλλά και άλλες που κυκλοφορούν στο εμπόριο ώστε να φανεί η αποτελεσματικότητά τους, με σκοπό να τις εμπιστευτούν και να τις χρησιμοποιούν οι χρήστες.

Θα πρέπει ακόμη να διερευνηθεί η δυνατότητα να ενσωματωθούν τέτοιες τεχνολογίες και εργαλεία, στα ήδη ενεργά και δημοφιλή κοινωνικά μέσα δικτύωσης, να υποστηρίζονται δηλαδή από τον πάροχο, διότι όπως αναφέραμε οι χρήστες δεν είναι πρόθυμοι να πληρώσουν για να τις αποκτήσουν, ακόμη κι αν πρόκειται για την ασφάλεια και τη προστασία τους.

Ακόμη μέσα από τους παράγοντες που αναφέραμε ότι επηρεάζουν τη χαμηλή υιοθέτηση των Pets, να σχεδιαστούν νέες τεχνολογίες που να ικανοποιούν τις ανάγκες των χρηστών, όπως την εύκολη χρήση, να ανταποκρίνονται γρήγορα και να παρέχουν ανατροφοδότηση για να βιώνουν οι χρήστες καταστάσεις άμεσα.

Τέλος θα μπορούσε να διερευνηθεί σε βάθος το Diaspora, που δεν είναι δημοφιλές δίκτυο κοινωνικής δικτύωσης και στηρίζεται σε κατανεμημένες βάσεις. Πρόκειται για μία κοινότητα και όχι μια εταιρεία όπως είναι το Facebook.

6.3 Επίλογος

Οι τεχνολογίες ενίσχυσης της Ιδιωτικότητας είναι επικουρικές, παρόλο που χρησιμοποιούμε PETs μπορούν να ξεφύγουν και να διαρρεύσουν προσωπικά δεδομένα, που θα κάνουν τους χρήστες να νιώσουν άβολα ή που μπορεί να χρησιμοποιηθούν από τρίτους για παραπλάνηση ή για να προκαλέσουν κακό.

Η προστασία της Ιδιωτικότητας και η ασφάλεια του καθενός είναι καθαρά προσωπική υπόθεση, γι' αυτό θα πρέπει να γίνεται ορθολογική χρήση των προσωπικών πληροφοριών που μοιραζόμαστε στα μέσα κοινωνικής δικτύωσης. Δεν υπάρχει πραγματική ασφάλεια, η καλύτερη ασφάλεια είναι να μην πεις κάτι.

Πρέπει να μάθουμε να αυτολογοκρινόμαστε και αυτό μπορούμε να το πετύχουμε μέσα από την εκπαίδευση. Η αυτολογοκρισία είναι μια στάση ζωής που πρέπει να καλλιεργηθεί από το σχολείο, στο πλαίσιο που με τα διάφορα ερεθίσματα που παρέχονται αναπτύσσεται και διαμορφώνεται ο χαρακτήρας του κάθε ανθρώπου.

Βιβλιογραφία

[01] Acquisti, A.(2010). The Economics of Personal Data and the Economics of Privacy, paper presented at Joint WPISP-WPIE Roundtable: The Economics of Personal Data and Privacy - 30 Years after the OECD Privacy Guidelines, Paris (France). Retrieved from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-oecd-22-11-10.pdf

[02] Anthonysamy, P. et al, (2011). Do the Privacy Policies Reflect the Privacy Controls on Social Networks?. In *Privacy, Security, Risk, and Trust, 2011 IEEE Third International Conference on Social Computing*, Boston, MA, USA, pp. 1155-1158.

[03] Bélanger, F., and Crossler, R.E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, *MIS Quarterly*, 35(4), 1017-1041.

[04] Bonneau, J., Preibusch, S.(2010). The Privacy Jungle: On the Market for Data Protection in Social Networks. In: *Economics of Information Security and Privacy*, pp. 121–167. Springer, US.

[05] Cavoukian, A. (2010). Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D.. *Identity in the Information Society*, 3(2), 247-251.

[06] Cheh, M. (2001). Technology and Privacy: Creating the conditions for preserving personal privacy. In: L. Sicilianos/M. Gavouneli (Eds.), *Scientific and Technological Developments and Human Rights*, Athen, pp. 103.

[07] Dammann, U., Simitis, S., EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997, pp. 67

[08] Edlin, A. S., & Harris, R. G. (2013). The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google. *Yale Journal of Law and Technology*, 15(2), 4.

[09] Fairchild, A., Ribbers, P.(2011). Privacy-Enhancing Identity Management in Business. In: Camenisch, J., Leenes, R., Sommer, D. (eds.) *Digital Privacy*. LNCS, vol. 6545, pp. 107–129. Springer, Heidelberg.

[10] Feigenbaum, J., Freedman, M.J., Sander, T., Shostack, A. (2002). Economic barriers to the deployment of existing privacy technologies (position paper). In: *Proceedings of the Workshop on Economics of Information Security*.

[11] Flash Eurobarometer 225: Data Protection in EU: Citizens' Perception. European Commission (2008)

[12] Hallinan, D., Friedewald, M., McCarthyb, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28(3), 263–272.

[13] Hill, K. (2013). Use Of Ad Blocking Is On The Rise. *Forbes.* Retrieved from http://www.forbes.com/sites/kashmirhill/2013/08/21/use-of-ad-blocking-is-on-the-rise/

[14] Jahid, Sonia, et al. (2012). DECENT: A decentralized architecture for enforcing privacy in online social networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on.* IEEE.

[15] Kobsa, A., Teltzrow, M.(2005). Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior. In: Martin, D., Serjantov, A. (eds.) PET 2004. LNCS, vol. 3424, pp. 329–343. Springer, Heidelberg.

[16] Laurie, G. T. (2002). Genetic privacy: a challenge to medico-legal norms, Cambridge University Press, 2002, pp. 60

[17] Leon, P.G., Ur, B., Balebako, R., Cranor, L.F., Shay, R., Wang, Y. (2012). Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising. In: *Proceedings of SIGCHI Conference on Human Factors in Computing Systems* (pp. 589–598). ACM, New York

[18] London Economics: Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission, DG Justice, Freedom and Security (2010)

[19] Madejskiy, M. et al. (2011).The Failure of Online Social Network Privacy Settings. *CUCS-010-11*, Retrieved from http://academiccommons.columbia.edu/catalog/ac:135406 .

[20] Meeder, B., Tam, J., Kelley, P.G. & and Cranor, L.F. (2010). RT @ IWantPrivacy: Widespread Violation of Privacy Settings in the Twitter Social Network, School of Computer Science, Carnegie Mellon University Pittsburgh, PA USA. Retrieved from http://www.cs.cmu.edu/~bmeeder/papers/Meeder-SNSP2010.pdf

[21] Nilizadeh, S., Jahid, S., Mittal, P., Borisov, N., & Kapadia, A. (2012). Cachet: a decentralized architecture for privacy preserving social networking with caching. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies* (pp. 337-348). ACM.

[22] Rodota, S. (2004). Privacy, Freedom, and Dignity - Closing Remarks at the 26th International Conference on Privacy and Personal Data Protection. *Wroclaw (16.09.2004).*

[23] Schwaig, K.S., Kane, G.C., Storey, V.C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information and Management*, 43(7), 805–820.

[24] Shin, D.H. (2010) The effects of trust, security and privacy in social networking: A security based approach to understand the pattern of adoption. *Interacting with Computers*, 22 (5), 428–438.

[25] SiliconIndia (2011). First anniversary of facebook 'LIKE' button. *siliconindia News*. Retrieved from http://www.siliconindia.com/shownews/First_anniversary_of_Facebook_LIKE_button-nid-82552-cid-1.html

[26] Simitis, S. (Hrsg.), Bundesdatenschutzgesetz-Kommentar, Baden-Baden 2006, pp. 136

[27] Solove, D.J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 479-564.

[28] Steel, E. , & Vascellaro, J. E. (2010). Facebook, Myspace Confront Privacy Loophole *The Wall Street Journal,* 21. Retrieved from http://online.wsj.com/news/articles/SB10001424052748704513104575256701215465596

[29] Strater, K., Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. In: *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1* (pp. 111–119). British Computer Society.

[30] Vemou, K., & Karyda, M. (2014). EMBEDDING PRIVACY PRACTICES IN SOCIAL NETWORKING SERVICES, Department of Information and Communication Systems Engineering, University of the Aegean, Samos.

[31] Vemou, K., & Karyda, M. (2013). A Classification of Factors Influencing Low Adoptionof PETs Among SNS Users. In *Trust, Privacy, and Security in Digital Business* (pp. 74-84). Springer Berlin Heidelberg.

[32] Wang, N., Grossklags, J., Xu, H. (2013). An Online Experiment of Privacy Authorization Dialogues for Social Applications. In: *Proceedings of the 2013 Conference on Computer SupportedCooperative Work,* CSCW 2013, pp. 261–272. ACM, New York.

[33] Wenstin, A. F. (1967). Privacy and Freedom, New York, pp. 7.

[34] Yao, M.Z. (2011). Self-Protection of Online Privacy: A Behavioral Approach. In: Trepte, S., Reinecke, L. (eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* Springer Berlin Heidelberg.

[35] Μήτρου, Λ. (2010). Η προστασία της Ιδιωτικότητας στην Πληροφορική και στις επικοινωνίες. Η νομική διάσταση. Στο: Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας (Επίμ.) *Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών,* Αθήνα: Παπασωτηρίου.

[36] http://cyberlaw.stanford.edu/wiki/index.php/PET

[37] http://www.goldenfrog.com/vyprvpn/buy-vpn?plan=annual

[38] http://www.purevpn.com

[39] https://diasporafoundation.org/

[40] https://www.tunnelbear.com/about/