

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Μηχανές αναζήτησης. Ζητήματα ασφάλειας και ιδιωτικότητας – Τεχνολογική και νομική διάσταση»

Δημήτριος Φρέσκας

M4090052

ΑΘΗΝΑ, ΣΕΠΤΈΜΒΡΙΟΣ 2012

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Μηχανές αναζήτησης. Ζητήματα ασφάλειας και ιδιωτικότητας – Τεχνολογική και νομική διάσταση»

Δημήτριος Φρέσκας

M4090052

Επιβλέπων Καθηγητής: Ευαγγελία Μήτρου

Εξωτερικός Κριτής: Βασίλειος Τσούμας

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΘΗΝΑ, ΣΕΠΤΈΜΒΡΙΟΣ 2012

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Πίνακας περιεχομένων

Ευχαριστίες....4

Περίληψη....5

Abstract....10

1.Εισαγωγή....14

2. Γενικές πληροφορίες για τις μηχανές αναζήτησης....16

2.1 Ιστορική αναδρομή....16

2.2 Τα είδη των μηχανών αναζήτησης....17

2.2.1 Η λειτουργία των μηχανών αναζήτησης με Crawler.....17

2.2.2 Η λειτουργία των μηχανών αναζήτησης με Καταλόγους.....18

2.2.3 Η λειτουργία των υβριδικών μηχανών αναζήτησης.....19

2.2.4 Η λειτουργία των μετά μηχανών αναζήτησης.....20

2.2.5 Η λειτουργία των στοχευμένων μηχανών αναζήτησης.....20

2.3 Ποιες είναι οι ποιο διαδεδομένες και γιατί.....21

3. Ιδιωτικότητα....24

3.1 Περιγραφή της ιδιωτικότητας....24

3.2 Αναφορά στα προσωπικά δεδομένα.....25

3.3 Νομοθετικό πλαίσιο εισαγωγή....26

3.4 Ιστορική αναδρομή στο Ευρωπαϊκό δίκαιο για την ιδωτικότητα....26

3.5 Περιγραφή της οδηγίας 95/46/ΕΚ76....27

3.6 Ομάδα εργασίας του άρθρο 29....29

3.7 Ελληνική Νομοθεσία....30

3.8 Αναδρομή στην δημιουργία νομικού πλαισίου περί της ιδιωτικότητας στις ΗΠΑ....33

3.9 Νομικό πλαίσιο των ΗΠΑ στο οποίο υπόκεινται εταιρείες μηχανών αναζήτησης....34

3.10 Τα αίτια δημιουργίας του safe Harbor....34

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4. Ιδιωτικότητα και μηχανές αναζήτησης 37

4.1 Τι δεδομένα <<συλλέγει >> μια μηχανή αναζήτησης κάθε φορά που επιλέγει να κάνει ο χρήστης μια αναζήτηση και τι επιπτώσεις έχει αυτό. 37

4.2 Η χρήση των πληροφοριών από τρίτα πρόσωπα 40

4.3 Οι πληροφορίες που συλλέγονται πως χρησιμοποιούνται και τι επιπτώσεις έχουν. 41

4.4 Διαρροή και ενοποίηση των πληροφοριών.....42

4.5 Διαρροή εμπιστευτικών πληροφοριών.....44

4.6 Μέθοδος : ανάλυση κίνησης 46

4.7 Θέματα ασφάλειας που προκύπτουν για τους χρήστες (και παραδείγματα που έχουν ήδη προκύψει).....47

4.8 Υπάρχουσες προβληματικές καταστάσεις (παράδειγμα google με την συνένωση του google search) 50

4.9 Η πολιτική απορρήτου της Google και άλλων εταιρειών 52

4.10 Οι ενέργειες της Ομάδα Εργασίας του Άρθρου 29 για την ιδιωτικότητα στις μηχανές αναζήτησης. 54

4.11 Προτεινόμενες μελλοντικές νομοθετικές τροποποιήσεις.....55

5.1 Εισαγωγή 60

5.2 Mixnet 60

5.2.1Σημεία ευπάθειας.....62

5.3 Crowds 63

5.3.1 Αρχές Λειτουργίας 64

5.3 Onion routing 67

5.3.1 Σημεία Ευπάθειας 70

5.5 Tor 70

5.6 Τεχνολογικές προτάσεις για καλύτερη διαχείριση των πληροφοριών ώστε να είναι χρηστικές αλλά και λιγότερο επικίνδυνες.....73

Βιβλιογραφία 78

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ευχαριστίες

Η παρούσα Διπλωματική Εργασία υλοποιήθηκε στο πλαίσιο των υποχρεώσεων μου για το μεταπτυχιακό πρόγραμμα «Πληροφοριακά Συστήματα» του Ο.Π.Α.

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου κα. Μήτρου Ευαγγελία., η οποία ως επιβλέπουσα καθηγήτρια της παρούσας Διπλωματικής Εργασίας μου παρείχε την πολύτιμη καθοδήγησή της σε όλα τα στάδια εκπόνησης της εργασίας καθώς και την αμέριστη ψυχολογική της υποστήριξη.

Τέλος, τις ευχαριστίες μου θα ήθελα να εκφράσω στους κοντινούς μου ανθρώπους και φίλους για την βοήθεια τους και την υπομονή τους κατά την συγγραφή της Διπλωματικής Εργασίας μου.

Περίληψη

Η εργασία αυτή περιγράφει κατά πόσο παραβιάζεται η ιδιωτικότητα των χρηστών των μηχανών αναζήτησης.

Αρχικά γίνεται μία ιστορική αναδρομή για την εξέλιξη των μηχανών αναζήτησης. Ποιο συγκεκριμένα πως από την Archie την πρώτη μηχανή αναζήτησης έγινε η μετάβαση στις ποιο σύγχρονες όπως το Google και την Yahoo.

Μετέπειτα γίνεται μία διάκριση ως προς την λειτουργία των μηχανών αναζήτησης και ποιο συγκεκριμένα στον τρόπο αναζήτησης και τον τρόπο ταξινόμησης των αποτελεσμάτων τους. Εκεί αναφέρονται πέντε βασικές κατηγορίες οι οποίες είναι οι εξής:

1. Μηχανές αναζήτησης Crawler.
2. Κατάλογοι.
3. Υβριδικές μηχανές αναζήτησης.
4. Μετά – μηχανές αναζήτησης.
5. Στοχευόμενες μηχανές αναζήτησης

Μετέπειτα αναφέρετε με στατιστικά στοιχεία και ποιες είναι και οι μηχανές αναζήτησης οι οποίες χρησιμοποιούνται περισσότερο και για ποιο λόγο επειδή γίνεται και ειδική αναφορά στις συγκεκριμένες για περιπτώσεις παραβίασης της ιδιωτικότητας αλλά για αναφορά στην πολιτική λειτουργίας που χρησιμοποιούν.

Αρχικά μία αναφορά στην ιδιωτικότητα. Ποιο συγκεκριμένα η ιδιωτικότητα σαν έννοια αντιμετωπίζετε διαφορετικά στην Ευρώπη από ότι στην Αμερική για αυτό και στην εργασία αναφέρονται δύο διαφορετικές απόψεις ως προς τον ορισμό της, το οποίο θα είναι χρήσιμο μετέπειτα για την ανάλυση των διαφορετικών νομικών πλαισίων που έχουν.

Βέβαια για την καλύτερη αντίληψη της ιδιωτικότητας αναφέρονται και τα είδη των προσωπικών δεδομένων αλλά και ποιο συγκεκριμένα των ευαίσθητων προσωπικών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δεδομένων . Μάλιστα γίνεται και αναφορά στο Ελληνικό νομικό πλαίσιο για το τι ακριβώς θεωρείτε ευαίσθητο προσωπικό δεδομένο.

Εν συνεχεία παρουσιάζεται το νομοθετικό πλαίσιο που υπάρχει στην Ευρωπαϊκή Ένωση. Ειδικότερα, αναφέρονται οι κοινοτικές οδηγίες που έχουν δημιουργηθεί για την προάσπιση της ιδιωτικότητας των χρηστών μίας μηχανής αναζήτησης. Για αυτό το λόγο γίνεται και μία ποιο λεπτομερή ανάλυση της κοινοτικής οδηγίας 95/46/ΕΚ76 η οποία αφορά το συγκεκριμένο θέμα.

Για την ρύθμιση της συγκεκριμένης οδηγίας και την τροποποίηση της ανάλογα με τις ανάγκες που προκύπτουν είναι υπεύθυνη η ομάδα εργασίας του άρθρο 29. Στην οποία γίνεται εκτενείς αναφορά για τον τρόπο λειτουργίας της καθώς και για τις προτάσεις της για τις μηχανές αναζήτησης αλλά και για τις μελλοντικές αλλαγές που έχει συστήσει για την προστασία της ιδιωτικότητας.

Για την ολοκλήρωση της έρευνας για το νομοθετικό πλαίσιο αναφέρεται πως οι κοινοτικές οδηγίες έχουν ενσωματωθεί στην ελληνική νομοθεσία (ποιοι νόμοι να φέρονται στην συγκεκριμένη οδηγία) και γίνεται αναφορά στην εποπτική αρχή η οποία είναι η αρχή προστασίας δεδομένων προσωπικού χαρακτήρα και πως αυτή λειτουργεί.

Η Ιδιωτικότητα, όπως αναφέρθηκε και παραπάνω, και τα πλαίσια της ορίζονται διαφορετικά στις ΗΠΑ από ότι στις χώρες της Ευρωπαϊκής ένωσης. Για το λόγο αυτό γίνεται και μία αναφορά στο νομικό πλαίσιο των ΗΠΑ για την ιδιωτικότητα και ειδικότερα για το safe harbor το οποίο έχουν αποδεχτεί εταιρείες που διαχειρίζονται τις γνωστότερες μηχανές αναζήτησης.

Ακολούθως γίνεται αναφορά κατά πόσο υπάρχει ή δεν υπάρχει ιδιωτικότητα όταν γίνεται μία αναζήτηση. Για την ανάλυση αυτή αναφέρεται αρχικά ποια στοιχεία συγκεντρώνει μια μηχανή αναζήτησης από ένα χρήστη.

Επίσης αναφέρεται πως αυτά τα στοιχεία μπορούν να τα συλλέξουν και τρίτοι και με ποιο σκοπό μπορούν να χρησιμοποιηθούν είτε από τους τρίτους είτε από τις ίδιες τις εταιρείες που διαχειρίζονται τις μηχανές αναζήτησης. Στο συγκεκριμένο σημείο της εργασίας γίνεται και η ανάλυση κινδύνων που μπορεί να υπάρξει από την συλλογή, ενοποίηση και επεξεργασία των προσωπικών του πληροφοριών για την ιδιωτικότητά του.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Οι κίνδυνοι για την ιδιωτικότητα των χρηστών αλλά και ο τρόπος που οι μηχανές συλλέγουν πληροφορίες φαίνεται και από τα παραδείγματα που αναφέρονται στην εργασία. Επίσης σκοπός των παραδειγμάτων είναι να δείξουν και πως οι συγκεκριμένες περιπτώσεις παράνομης και αυθαίρετης περισυλλογής πληροφοριών αντιμετωπίστηκαν από την αντίστοιχες αρχές.

Επειδή σύμφωνα και με τα στοιχεία που έχουν προαναφερθεί , η Google είναι η ποιο διάσημη μηχανή αναζήτησης, γίνεται και μία ειδική αναφορά στον τρόπο λειτουργίας και ποια στοιχεία συλλέγει. Ακόμα αναφέρεται και περιπτώσεις που έχουν απασχολήσει τους χρήστες για την παραβίαση της ιδιωτικότητάς τους. Ειδικότερα γίνεται και μία ανάλυση για την ενοποίηση των υπηρεσιών με την οποία επιτυγχάνει μεγαλύτερη συλλογή πληροφοριών του χρήστη και άρα μπορεί να αυξήσει την πιθανότητα παραβίασης της ιδιωτικότητάς του.

Στη συνέχεια παρουσιάζεται και η πολιτικές που ακολουθούνται από τις εταιρείες των μηχανών αναζήτησης και πως αυτές μπορούν να προασπίσουν τα δικαιώματα του χρήστη αλλά και των ίδιων των εταιρειών.

Για την ολοκλήρωση της μελέτης της ιδιωτικότητας και της προάσπισης του από της αρχές, αναφέρονται οι μελέτες και οι προτάσεις της Ομάδα Εργασίας του Άρθρου 29 που έχουν γίνει μέχρι τώρα και αφορούν την συμπεριφορά των μηχανών αναζήτησης ως προς την συλλογή πληροφοριών των χρηστών τους.

Ιδιαίτερη σημασία για το κομμάτι που αναφέρεται στο νομικό πλαίσιο στην εργασία αυτή έχουν και οι προτάσεις που έχουν γίνει από την Ομάδα Εργασίας του Άρθρου 29 και αφορούν μελλοντικές αλλαγές που πρέπει να γίνουν για την περαιτέρω προάσπιση της ιδιωτικότητας των χρηστών.

Υπάρχουν αρκετές τεχνολογίες ανωνυμίας που έχουν εφαρμοστεί και δοκιμαστεί στην διαδικτυακή περιήγηση. Οι πιο διαδομένες είναι οι mix network(mixnet), crowds, onion routing και tor. Η καλύτερη λύση για μια ασφαλή και ανώνυμη περιήγηση είναι ένα σύστημα ικανό να διασφαλίσει την ιδιωτικότητα χωρίς να επηρεάζει την ποιότητα της υπηρεσίας, καθώς πολλές από αυτές έχουν υπολογιστικό κόστος. Αυτό έχει σαν αποτέλεσμα την εμφάνιση καθυστέρησης κατά την διάρκεια της περιήγησης.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Το 1981, προτάθηκε ένα ανώνυμο κανάλι επικοινωνίας, βασισμένο στην κρυπτογραφία και στην μεταλλαγή το οποίο ονομάστηκε mix networks (mixnet). Το mixnet είναι ένα πολύ-επίπεδο σύστημα που δέχεται ένα σύνολο από εισόδους και παράγει μια έξοδο από σύνολα που περιέχουν την είσοδο κρυπτογραφημένη και μεταλλαγμένη.

Επιπροσθέτως, το Crowds επιτρέπει την ανάκτηση πληροφοριών από το διαδίκτυο χωρίς να εκθέτει πληροφορίες της ιδιωτικότητας σε τρίτους. Στόχος του Crowds είναι η ανώνυμη περιήγηση, ούτος ώστε είτε η πληροφορία που αφορά τον χρήστη, είτε η πληροφορία που ανακτάται από το δίκτυο, να παραμένει κρυφή από άλλους. Το Crowds βασίζεται στο ότι κάποιος μπορεί να εξασφαλίσει την ανωνυμία του όταν βρίσκεται μέσα στο πλήθος.

Επίσης μία από τις βασικές τεχνολογίες ανωνυμοποιήσης είναι και το Onion routing. Το Onion routing αποτελεί μια γενικού σκοπού υποδομή για ιδιωτικές συνδέσεις σε ένα δημόσιο δίκτυο μεταφοράς δεδομένων. Παρέχει ανώνυμες συνδέσεις χρησιμοποιώντας διαφορετικά επίπεδα κρυπτογράφησης που είναι ιδιαίτερα ανθεκτικά σε επιθέσεις τύπου παρακολούθησης και ανάλυσης κίνησης. Οι συνδέσεις είναι αμφίδρομες, σχεδόν πραγματικού χρόνου και μπορούν να χρησιμοποιηθούν είτε για κινήσεις προσανατολισμένες σε σύνδεση, είτε για κινήσεις άνευ εγκατάστασης σύνδεσης.

Τέλος το Tor δίκτυο είναι βασισμένο στο onion-routing όπου η κίνηση προωθείτε μέσω πολλαπλών δρομολογητών κρυπτογραφημένη. Το μονοπάτι μέσα στο δίκτυο είναι έτσι φτιαγμένο ούτως ώστε κάθε δρομολογητής να γνωρίζει μόνο τον προηγούμενο και τον επόμενο. Στην πραγματικότητα ο πρώτος δρομολογητής γνωρίζει την πηγή της πληροφορίας και ο τελευταίος τον προορισμό. Παρόλα αυτά, αν και οι δυο αυτοί δρομολογητές συνεργαστούν, μπορούν να εκτιμήσουν την κίνηση της πληροφορίας. Οι tor δρομολογητές εγγράφονται σε μία λίστα. Κάθε δρομολογητής αναφέρει την IP του, το δημόσιο κλειδί του, την πολική που θα ακολουθήσει σε σχέση με την κίνηση που θα δεχτεί και σε ποια ταχύτητα.

Μέχρι τώρα όλες οι τεχνολογίες ανωνυμοποίησης όπως το Tor δεν είναι κλιμακούμενες, και απαιτούν από τους χρήστες να διατηρούν ενημερωμένες πληροφορίες για όλους τους διαθέσιμους Tor- συνεργάτες του συστήματος. Στην παρούσα εργασία παρουσιάζετε μία κλιμακωτή ανώνυμη επικοινωνία

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συμπεριλαμβάνοντας μια προσέγγιση P2P. Αναλύεται μία PIR-Tor αρχιτεκτονική βασισμένη στο Tor, κατά την οποία οι χρήστες αποκτούν πληροφορίες μόνο για λίγους onion δρομολογητές χρησιμοποιώντας private information retrieval (PIR) τεχνικές. Πιο συγκεκριμένα στο Tor δίκτυο που παρουσιάζεται απαιτείται οι χρήστες να γνωρίζουν μόνο για 3 συνεργάτες ούτως ώστε να εδραιώσουν μια ανώνυμη επικοινωνία. Αυτή η ελάχιστη απαίτηση σε πληροφορίες για τους onion δρομολογητές μας εξασφαλίζει την επιθυμητή επεκτασιμότητα ενώ μέσω των PIR τεχνικών επιτυγχάνεται και η ανωνυμία του χρήστη.

Συμπερασματικά, και από την παρουσίαση των παραπάνω στην εργασία η ευθύνη για την προστασία της ιδιωτικότητας θα μπορούσε ξεκινάει από τον ίδιο τον χρήστη. Αυτό θα ήταν όμως σχεδόν αδύνατο, λόγο τον γνώσεων του μέσου χρήστη για τις επιπτώσεις που θα είχαν οι επιλογές του και οι ενέργειές του. Έτσι μετά την ανάλυση του νομικού πλαισίου και των περιπτώσεων που έχουν προκύψει θα μπορούσε να θεωρηθεί ότι το νομικό πλαίσιο μπορεί να προασπίσει τα δικαιώματα των χρηστών και να προλαμβάνει κάποιες από τις μελλοντικές περιπτώσεις. Για την καλύτερη όμως πρόληψη αλλά και για μία ανώνυμη περιήγηση στον παγκόσμιο ιστό σημαντικό ρόλο έχει και η παράλληλη ανάπτυξη των τεχνολογιών ασφάλειας και ανωνυμίας όσο οι μηχανές αναζήτησης δημιουργούν νέες μεθόδους για να συλλέγουν δεδομένα για τους χρήστες τους.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Abstract

This assignment describes to what extent privacy of search engine users is violated.
Initially there is a historical explanation of the development of search engines, and more specifically how search engines were developed, starting with Archie, the first search engine, and ending in more modern search engines such as Google and Yahoo.
Following this is an explanation of the operation of search engines and more specifically the way in which searches are conducted and the way in which their results are organized. There we refer to five basic categories, which are as follows:

1.Search engine crawlers
2.Catalogues
3.Hybrid search engines
4.Meta-search engines
5.Targeted search engines.

Next, we refer with statistical data to which search engines are the most used and for what reason, because there is are references to specific cases of the violation of privacy by search engines but also to the operational policy which they use.
Initially a reference to privacy. More specifically, privacy as a concept is dealt with differently in Europe as it is in America, and for this reason two different aspects are referred to in terms of its definition, which will be useful later in the different legal frameworks that Europe and America have.
In order to better understand privacy, the different types of personal data are also referenced, but more specifically the nature of sensitive personal data. Also referenced is the Greek legal framework regarding what exactly is considered sensitive personal information.
Then the legal framework that currently exists in the European Union is presented. There are references to the community directives that have been produce for the protection of privacy of the users of search engines. For this reason there is a detailed analysis of Directive 95/46/EC76 which refers to this specific subject.

Regarding the regulations in this directive and modifications to it depending on the needs that exist, the workgroup for article 29 is the responsible organization, to which

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

extensive references are made regarding its method of operation as well as its suggestions regarding search engines and future changes for the protection of privacy.

For the completion of the research on legislative framework, it is shown that the community directives have been assimilated Greek legislation (and which laws are brought in from the specific directive), and there is a reference to the supervisory authority, which is the principle of the protection of data of a personal nature, and how it operates.

Privacy, as mentioned above, and its relevant frameworks are defined differently in America than how they are defined in the countries of the European Union. For this reason that is also reference to the legal framework of the United States regarding privacy and especially the Safe Harbor framework which has accepted companies that manage the better known search engines.

Furthermore, there is significant attention paid to the question of how much privacy the user has or does not have when they conduct a search via a search engine. For this analysis the research shows with data a search engine collects from a user.

As well as this, it is shown how these data can be collected by third parties and with which aims they can be used either by third parties or by the companies that manage search engines. On this specific point, there is also an analysis of the dangers to a user's privacy that can exist as a result of the collection, consolidation and processing of personal data.

Dangers to the privacy of users but also the way in which search engines collect information is also shown by the examples that are referred to in the work. As well as this the aim of the examples is to show how these specific cases of illegal and arbitrary collection of data were dealt with by the corresponding authorities.

Because, according the evidence that has been presented, Google is the most widely-used search engine, special reference is made to the way in which it operates and what information it collects. Also certain cases that have concerned users regarding their privacy have also been referred to. As well as this there is an analysis of the consolidation of services through which a larger collection of user information is accelerating, hence the increase in the chances of a user's privacy being violated.

In continuing, the policies that search engine companies follow are also presented, as well as how they can protect the rights of both the user and the company itself.

For the completion of the study of privacy and the protection of it by authorities, the studies and suggestions of Workgroup of Article 29 have also been referred to that

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

have taken place until now and they concern the behaviour of search engines in terms of their collection of user information.

Special importance is given to the part of the research related to the legal framework and the suggestions that have been put forward by the Workgroup of Article 29 and concern the future changes that must happen for the further protection of the privacy of users.

There are many technologies regarding anonymisation which have been applied and tested on internet browsing. The most widespread of these are mix networks (mixnet), Crowds, onion routing and tor. The best solution for safe and anonymous browsing would be a system able to secure privacy without affecting the quality of service, whilst many of them have a computing cost. This appears in the form of delays during browsing.

In 1981, it was suggested that there be an anonymous channel of communication, based on cryptography and alteration, which was named mix networks (mixnet). Mixnet is a multi-level system which accepts an aggregation of inputs and produces an output from aggregations which contain the cryptographically encoded and altered input.

In addition, Crowds allows for the retrieval of information from the internet without exposing privacy information to third parties. The aim of Crowds is to achieve anonymous browsing, whilst both the information concerning the user, and the information retrieved from the internet, remain hidden from others. Crowds is based on the fact that someone can secure his anonymity when found amongst a mass of information.

As well as this, one of the basic anonymisation technologies is Onion routing. Onion routing constitutes a general-purpose infrastructure for private connections to a public data network. It provides anonymous connections using various levels of cryptography, which are especially resistant to monitoring attacks and traffic analysis. The connections are bidirectional, almost real time, and can be used either for connection oriented movements, or movements without and installed connection.

Finally, the Tor network is based on onion-routing when movement is forwarded through multiple routers. The path inside the network is designed so that each router only recognizes the previous and following routers. In reality the first router is aware of the source of the information and the last one is aware of the destination. Despite this, if both routers cooperate, they can evaluate the movement of information. Tor

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

routers are written in a list. Each router states its IP, public key, and the policy it will follow in relation to the motion it will detect and at which speed.

Until now all the anonymisation technologies such as Tor are not scaleable, and require from their users that they maintain updated information on all available Tor co-operators in the system. Presented in this paper is a scalable anonymous communication system, using a P2P approach. A PIR-Tor architecture based on Tor is also analysed, through which users obtain information on a few onion routers using private information retrieval techniques(PIR). More specifically, in the Tor network that is presented, users are required to be aware of only three co-operatives in order to maintain anonymous communication. This minimal requirement for information for onion routers secures the desired scalability whilst through PIR techniques the anonymity of the users is maintained.

In conclusion, and from the presentation of the above in the project, the responsibility from privacy could start from the user himself. That however would be almost impossible, due to the lack of knowledge that the average user has regarding the consequences of his choices and actions. Thus, after the analysis of legal frameworks and cases which have come about it could be considered that the legal framework can protect the rights of the user and prevent some possible future possible cases. For the best prevention but also to achieve anonymous web browsing on the world wide web it is also important to consider the simultaneous development of security technologies and anonymity as search engines formulate new methods to collect data on their users.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

1.Εισαγωγή

Τα τελευταία χρόνια το μέγεθος της διαθέσιμης πληροφορίας μέσω διαδικτύου αυξάνεται με ιλιγγιώδεις ρυθμούς. Οι περισσότεροι χρήστες αναζητούν πληροφορίες σε οποιασδήποτε μορφή (π.χ. εικόνες, κείμενα, βίντεο), για τους δικούς τους προσωπικούς σκοπούς. Η αναζήτηση αυτή θα ήταν πραγματικά ανέφικτη εάν δεν υπήρχαν εφαρμογές και προγράμματα όπως οι μηχανές αναζήτησης. Μάλιστα σήμερα πολλές από αυτές θεωρούνται από τις πιο διαδομένες σελίδες παγκοσμίως.

Η διαδικτυακή αναζήτηση γίνεται πλέον από πολλές και διαφορετικές μηχανές αναζήτησης οι οποίες λειτουργούν με ιδιαίτερο σύστημα λειτουργίας, καθώς και με την δική της πολιτική - τεχνολογική προστασία δεδομένων.

Το κοινό που έχουν οι μηχανές αναζήτησης είναι πλέον κάποια συγκεκριμένα δεδομένα που διατηρούν στις βάσεις τους. Στην συγκεκριμένη εργασία αναλύεται την εξέλιξη των τεχνολογικών δυνατοτήτων των μηχανών αναζήτησης στην συγκέντρωση πληροφοριών για τους χρήστες τους.

Επίσης θα αναλυθεί ο λόγος για τον οποίο μία μηχανή αναζήτησης συγκεντρώνει τις συγκεκριμένες πληροφορίες, που μπορεί να τις διανέμει και με ποιον σκοπό και κατά πόσο αυτό παραβιάζει τον ιδιωτικό βίο των χρηστών. Κατά πόσο οι πολιτικές προστασίας που ακολουθούν οι συγκεκριμένες εταιρείες και οι τρόποι διαχείρισης των πληροφοριών που διαθέτουν εναρμονίζονται με τα νομικά πλαίσια των ΗΠΑ αλλά και της ΕΕ ώστε να γίνει μία σύγκριση περί του τι θεωρείτε ιδιωτικότητα σε διαφορετικές χώρες αλλά και πως αντιμετωπίζουν οι νομοθετικοί θεσμοί. Τα ‘δημόσια’ πλέον, δεδομένα μπορούν να χρησιμοποιηθούν είτε από τους ιδιοκτήτες των μηχανών αναζήτησης είτε από τρίτους, με συγκεκριμένους τρόπους που θα αναλυθούν στην παρούσα εργασία, ούτος ώστε να εξυπηρετήσουν δικούς τους σκοπούς παραβιάζοντας την ιδωτικότητα του χρήστη.

Για την παραπάνω σύγκριση θα αναφερθούν αναλυτικά τα υπάρχοντα νομοθετικά πλαίσια για την προστασία του χρήστη αλλά και οι κατάλληλες τεχνολογικές μέθοδοι ασφάλειας για την προστασία της ιδιωτικότητάς του.

Κυρίως στόχος της εργασίας είναι η ανάδειξη των τεχνολογικών και των νομοθετικών λύσεων που προτείνονται για την διασφάλιση της ιδιωτικότητας των

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

χρηστών μιας μηχανής αναζήτησης Κατά πόσο η καινοτομία της τεχνολογίας έχει αντίκτυπο στον ιδιωτικό βίο και στην ιδιωτικότητα του χρήστη και ποια είναι τα όρια ασφάλειας που τίθενται από τα νομοθετικά και τις τεχνολογικές δυνατότητες.

Τέλος θα γίνουν κάποιες προτάσεις, τόσο τεχνολογικές όσο και νομοθετικές, οι οποίες θα προλαμβάνουν τέτοιου είδους μελλοντικά φαινόμενα παραβίασης της ιδιωτικότητας.

2. Γενικές πληροφορίες για τις μηχανές αναζήτησης

2.1 Ιστορική αναδρομή

Πριν να υπάρξει κάποια από τις γνωστές μηχανές αναζήτησης η πλειοψηφία των ιστοσελίδων λειτουργούσαν μέσω του πρωτοκόλλου μεταφοράς αρχείων (FTP). Ωστόσο, έπρεπε να ξέρει ο χρήστης που βρίσκονταν τα αρχεία για να μπορεί να έχει πρόσβαση . Παρατηρώντας τις ανάγκες και λόγο του συνεχούς αυξανόμενου όγκου της πληροφορίας στον παγκόσμιο ιστό, δημιουργήθηκε μία πρώτη μορφή μηχανής αναζήτησης που λεγόταν Archie η οποία δημιουργήθηκε από τον Peter Deutsch, Alan Image, και τον Bill Wheelan. Το μειονέκτημα σε αυτήν την μηχανή αναζήτησης ήταν ότι ο χρήστης που για να μπορέσει να βρει ένα συγκεκριμένο αρχείο θα έπρεπε να ήξερε ακριβώς το όνομα του αρχείου.

Η ιδέα αύτη όμως θα εξελισσόταν και έτσι δημιουργήθηκε η Veronica, ένα σύστημα το οποίο χρησιμοποιούταν να ψάχνει για αρχεία κειμένου σε ιστοσελίδες Gopher, και όχι μόνο αλλά και για εικόνες και άλλα είδη αρχείων τα οποία ήταν στις ιστοσελίδες FTP. Μετά όμως το διαδίκτυο εξελίχθηκε ώστε να χρειάζεται ένα πιο περίπλοκο σύστημα αναζήτησης. Αυτό πήρε μορφή με το σύστημα που λεγόταν World Wide Web Wanderer, το οποίο έβρισκε ΕΕΠ και τους έβαζε σε μία βάση δεδομένων, στο οποίο μπορούσε να αναζητείται κάποια κατάλληλη ιστοσελίδα πιο εύκολα και γρήγορα. Το ALIWEB αποτελούσε ένα όμοιο εργαλείο, αλλά χρησιμοποιούσε πληροφορίες από αυτούς που παρήγαγαν τις ιστοσελίδες.

Αυτό βέβαια δεν μπορούσε να λειτουργεί μακροχρόνια – ο όγκος των ιστοσελίδων αυξανόταν συνεχώς και τα ήδη υπαρχών εργαλεία θα ήταν αναποτελεσματικά. Δημιουργήθηκαν συστήματα ποιο εξελιγμένα συστήματα που χρησιμοποιούσαν «αράχνες». Αυτές οι «αράχνες» έψαχναν πληροφορίες από ιστοσελίδες και δημιουργούσαν τις δικές τους λίστες για να τις βάλουν σε βάσεις δεδομένων. Αυτά τα συστήματα όμως ήταν πολύ απλά. Το Yahoo!, όταν φτιάχτηκε από δυο φοιτητές στο Πανεπιστήμιο Stanford που χρησιμοποιούσαν τέτοια συστήματα με αράχνες και βάζανε τις πληροφορίες σε χειροποίητες λίστες. Αυτό όμως ήταν και αυτή τη φορά ένα πολύ απλό σύστημα που δεν επαρκούσε για την τεράστια ποσότητα κίνησης που τελικά αναπτυσσόταν όσο αυξανόταν η χρήση του διαδικτύου[i].

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.2 Τα είδη των μηχανών αναζήτησης

Παρατηρώντας τα παραπάνω ιστορικά στοιχεία γίνεται αντιληπτό ότι οι μηχανές αναζήτησης είναι ένας συνεχώς αναπτυσσόμενος τομέας του παγκοσμίου ιστού. Για αυτό το λόγο έχουν δημιουργηθεί πλέον και πολλές και διαφορετικές μηχανές αναζήτησης , κυρίως ως προς τον τρόπο αναζήτησης. Έτσι μπορούμε να αναφέρουμε ότι υπάρχουν πέντε κύρια είδη μηχανών αναζήτησης τα οποία είναι τα εξής[ii]:

6. Μηχανές αναζήτησης Crawler.
7. Κατάλογοι.
8. Υβριδικές μηχανές αναζήτησης.
9. Μετά – μηχανές αναζήτησης.
10. Στοχευόμενες μηχανές αναζήτησης.

2.2.1 Η λειτουργία των μηχανών αναζήτησης με Crawler.

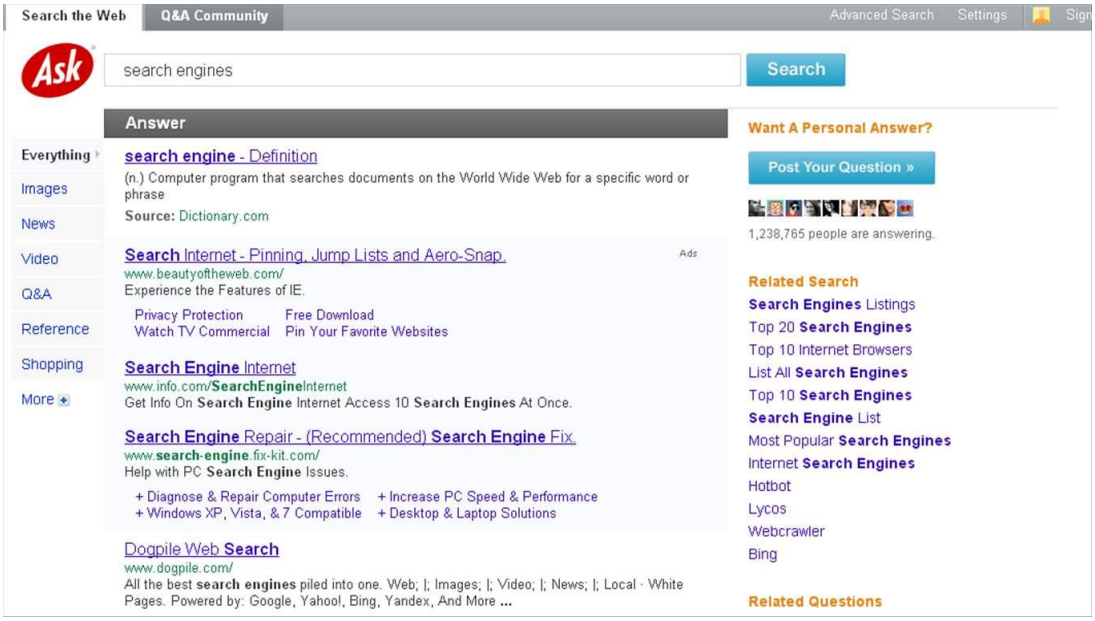
Αρχικά θα αναφερθούμε στις crawler based οι. Το κύριο χαρακτηριστικό τους είναι τα προγράμματα κατηγοριοποιήσεις των σελίδων που θα έχουν σαν αποτελέσματα , μετά από μία αναζήτηση, και ονομάζονται crawler, bot ή spider.

Αρχικά ο χρήστης θα θέσει μία λέξη ή πρόταση κλειδί και μετά η μηχανή θα εξερευνήσει τον παγκόσμιο ιστό για να βρει κάποιες σελίδες που θα τις θεωρήσει κατάλληλες. Αυτό γίνεται συνήθως με ανάθεση βαρών. Δηλαδή εάν μία σελίδα εμφανίζει τη λέξη κλειδί στο url της ή στο κείμενο της ή ακόμα και στους συνδέσμους στους οποίους περιέχει. Εν συνεχεία τις σελίδες αυτές θα τις αποθηκεύσει στην βάση δεδομένων που έχει η μηχανή για μελλοντικές αναζητήσεις. Έτσι γίνεται μία κατηγοριοποίηση των σελίδων ανά θέμα και κάθε φορά που ένας χρήστης κάνει μία αναζήτηση, με το ίδιο θέμα του επιστρέφονται αποτελέσματα από τη βάση δεδομένων της μηχανής αναζήτησης. Στην βάση αυτή προσθέτονται συνέχεια νέες σελίδες επειδή οι crawler κάνουν συνεχείς αναζητήσεις. Βέβαια μπορεί και να αφαιρεθούν και σελίδες που ήταν σχετικές με την λέξη κλειδί αλλά έχουν

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πάψει πλέον να είναι επειδή έχει αλλάξει το περιεχόμενό τους. Μία από τις ποιό γνωστές μηχανές σε αυτήν την κατηγορία είναι η ask.com.

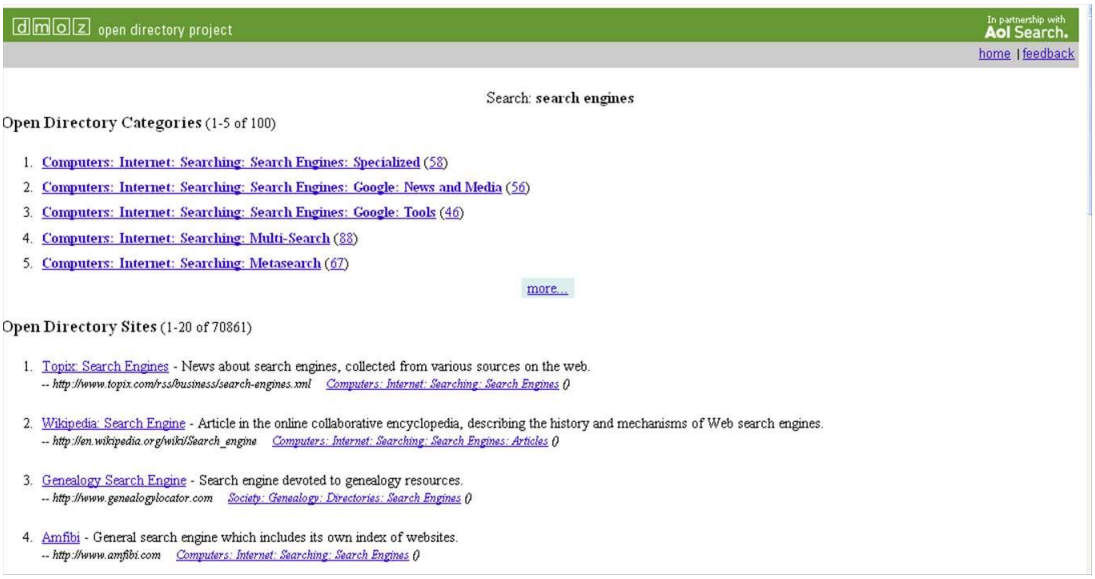
Παρακάτω μπορούμε να παρατηρήσουμε την μορφή αποτελεσμάτων από μία μηχανή αναζήτησης crawler .



Εικόνα 1 πηγή: ask.com

2.2.2 Η λειτουργία των μηχανών αναζήτησης με Καταλόγους.

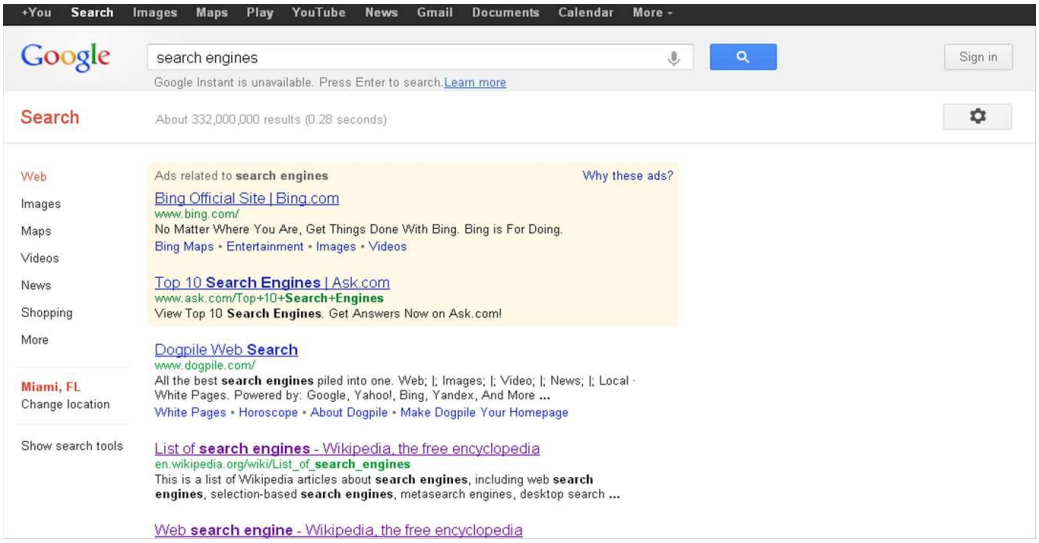
Το ιδιαίτερο σε αυτήν την κατηγορία μηχανών αναζήτησης είναι ότι ο διαχειριστής παρεμβαίνει για την κατηγοριοποίηση των σελίδων. Έτσι υπάρχουν κάποιοι διαχειριστές που διασχίζουν τις σελίδες και ανάλογα με το αντικείμενό τους τις κατατάσσουν και τις αποθηκεύουν σε μία βάση δεδομένων σε κατηγορίες. Ώστε όταν ο χρήστης αναζητήσει με την αντίστοιχη λέξη κλειδί κάποιες σελίδες σαν αποτέλεσμα θα του επιστραφούν οι σελίδες που είναι στην συγκεκριμένη κατηγορία.dmoz.org.



Εικόνα 2 πηγή: dmoz.org

2.2.3 Η λειτουργία των υβριδικών μηχανών αναζήτησης.

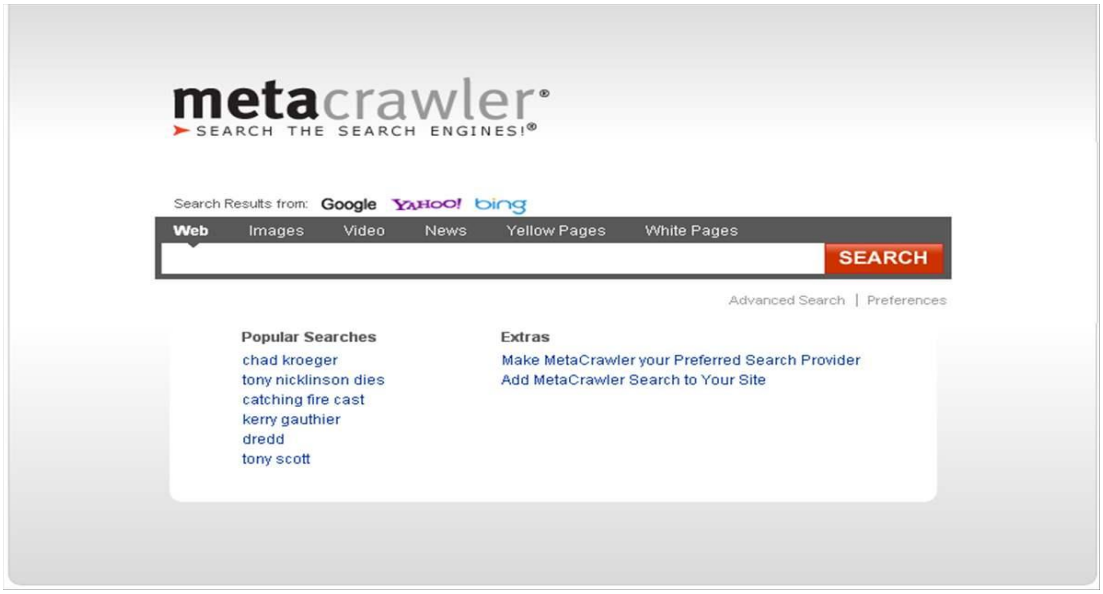
Αυτή η κατηγορία περιλαμβάνει ένα συνδυασμό των δύο παραπάνω κατηγοριών. Εδώ θα δούμε ότι οι κατηγορίες δημιουργούνται από crawler αλλά την τελική κατάταξη την κάνουν οι διαχειριστές. Οι ποιο γνωστές μηχανές σε αυτή την κατηγορία είναι οι: yahoo.com,google.com



Εικόνα 3 πηγή: google.com

2.2.4 Η λειτουργία των μετά μηχανών αναζήτησης.

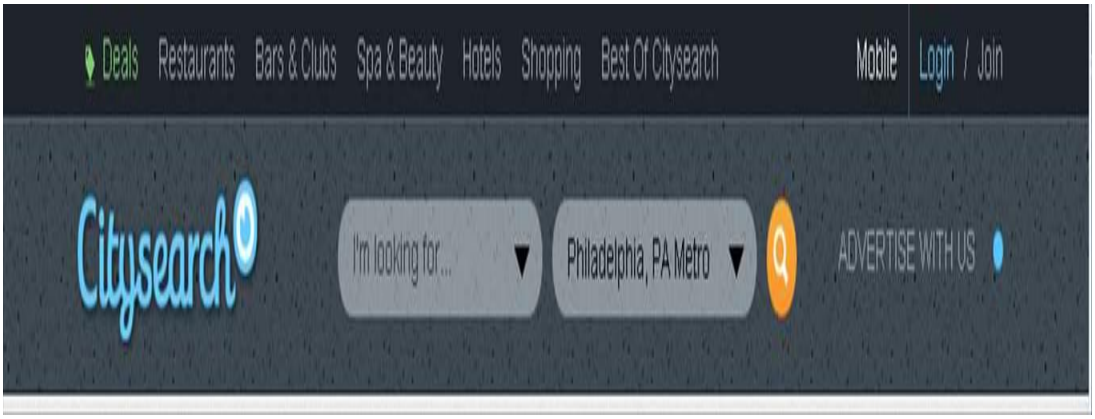
Οι μετά μηχανές αναζήτησης ουσιαστικά κάνουν μία αναζήτηση και τελικά μια κατηγοριοποίηση ανάμεσα στα αποτελέσματα, για την ίδια λέξη κλειδί, μεταξύ των αποτελεσμάτων διαφόρων μηχανών αναζήτησης. Συνήθως η τελική κατηγοριοποίηση στηρίζεται στην επισκεψιμότητα που έχουν οι σελίδες. Μία αρκετά γνωστή μηχανή μετά αναζήτησης είναι η Metacrawler



Εικόνα 4 πηγή: metacrawler.com

2.2.5 Η λειτουργία των στοχευμένων μηχανών αναζήτησης.

Με τις στοχευόμενες μηχανές αναζήτησης ένας χρήστης μπορεί να κάνει αναζητήσεις μόνο σε συγκεκριμένους θεματικούς καταλόγους. Εδώ έχει γίνει μια συγκέντρωση ιστοσελίδων είτε με crawler είτε με υβριδικές μεθόδους. Οι κυριότερες κατηγορίες σε αυτές τις μηχανές είναι εκπαιδευτικές κατηγορίες, πληροφορίες για ταξιδιωτικούς προορισμούς, είδη μουσικής και άλλα. Μια από τις διασημότερες σελίδες σε αυτήν κατηγορία των ιστοσελίδων είναι η Citysearch



Εικόνα 5 πηγή: citysearch.com

Από τις παραπάνω εικόνες ότι οι περισσότερες μηχανές έχουν την ίδια λογική ως προς την δομή τους. Έτσι ο χρήστης γράφει την λέξη κλειδί και η μηχανή παρουσιάζει σε μορφή συνδέσμων τα αποτελέσματα. Επίσης μπορούμε να παρατηρήσουμε ότι υπάρχει η επιλογή της δημιουργίας λογαριασμού για τον χρήστη και της ενεργοποίησης κατά την είσοδό του.

2.3 Ποιες είναι οι ποιο διαδεδομένες και γιατί.

Από την εικόνα (6) γίνεται αντιληπτό ότι η google κατέχει μακράν το μεγαλύτερο κομμάτι της αγοράς και ακολουθεί η yahoo. Η τεράστια αυτή διαφορά οφείλεται σε συγκεκριμένους λόγους.

Αρχικά θα μπορούσαμε να αναφέρουμε ότι έχει γίνει η πιο διάσημη μηχανή αναζήτησης, σχεδόν όλοι οι χρήστες στον κόσμο την αναγνωρίζουν, και αυτό οφείλεται και στο τμήμα προώθησης που έχει το οποίο αναγνωρίζεται σαν ένα από τα κορυφαία στον κόσμο.

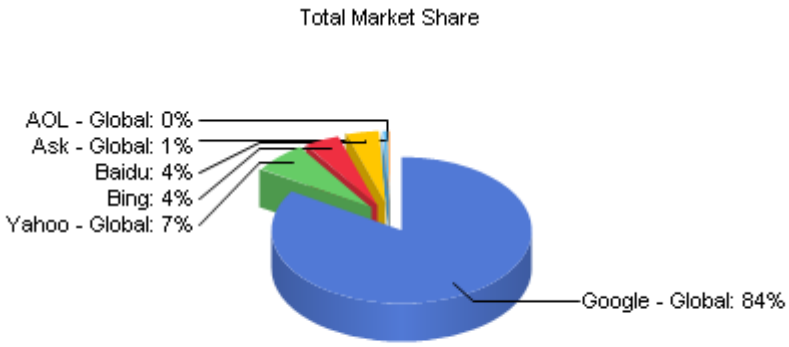
Επίσης ο αλγόριθμος που χρησιμοποιεί έχει από τα καλύτερα αποτελέσματα σε αναζητήσεις σε σύγκριση με τις άλλες μηχανές. Εδώ πρέπει να γίνει αναφορά και στον χρόνο επιστροφής αποτελεσμάτων που συγκριτικά με όλες τις υπόλοιπες μηχανές είναι ο μικρότερος. Ακόμα το πλήθος των αναζητήσεων μπορεί να είναι πολύ μεγάλο γιατί υποστηρίζει ένα τις περισσότερες γλώσσες στων κόσμο.

Το περιβάλλον που έχει για αρχική σελίδα το κάνει αυτόματα πολύ φιλικό για τους αρχάριους χρήστες γιατί το διακρίνει η απλοϊκότητα του. Εδώ πρέπει να αναφερθεί ότι ο χρήστης μπορεί να επιλέξει και να παραμετροποιήσει ακόμα και την εμφάνιση της σελίδας του google Βέβαια μπορεί να βοηθήσει και τους υπόλοιπους χρήστες με την ένδειξη προτεινόμενων αναζητήσεων κατά την διάρκεια πληκτρολόγησης της λέξης ή της φράσης κλειδιού.

Τέλος τα αρχεία που μπορεί να αναζητήσει κάποιος είναι ακόμα και σε εικόνες βίντεο, χάρτες, ειδήσεις και άλλα εκτός από ιστοσελίδες και κείμενα.

Search Engine Market Share

July, 2012



Search Engine	**Total Market Share**
Google - Global	83.06%
Yahoo - Global	6.71%
Bing	4.27%
Baidu	3.97%
Ask - Global	0.51%

AOL - Global	0.31%
Excite - Global	0.02%
Lycos - Global	0.01%
AltaVista - Global	0.00%

Εικόνα 6 πηγή: http://www.netmarketshare.com

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3. Ιδιωτικότητα

3.1 Περιγραφή της ιδιωτικότητας

Η ιδιωτικότητα είναι μία έννοια που προσδιορίζεται διαφορετικά και ειδικότερα ανάμεσα σε Ευρώπη και στην Αμερική όπου υπάρχουν και διαφορετικές νομοθεσίες για την προστασία της. Έτσι για την Ευρώπη θα μπορούσαμε να αναφερθούμε με τον συγκεκριμένη περιγραφή:

Η παραπομπή στην περίφημη συνηγορία των αμερικανών δικαστών Warren και Brandeis (1896) υπέρ του δικαιώματος του ατόμου σε μία ανενόχλητη ιδιωτική ζωή (the right to be let alone) 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 – ήδη η «κλασική» 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 ελαχιστοποίηση των "παρεμβάσεων" (intrusiveness), η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς, της – υπό στενή έννοια - ιδιωτικότητας (intimacy), της ανωνυμίας και της απόσυρσης (reserve)[iii].

Στην Αμερική η έννοια της ιδιωτικότητας, έννοια δύσκολη ως προς τον ορισμό και την τήρησή της, στην ψηφιακή εποχή αναφέρεται με διαφορετικό τρόπο. Στο χώρο του παγκόσμιου ιστού το ιδιωτικό γίνεται συχνά δημόσιο και μάλιστα πολλές φορές οικειοθελώς. Άρα το υποτιθέμενο δίλημμα προστασία των προσωπικών δεδομένων και ασφάλεια, ελευθερία του λόγου και προάσπιση της ιδιωτικότητας μάλλον καταρρίπτεται.

Η ελευθερία της έκφρασης και η ασφάλεια, στον παγκόσμιο ιστό είναι έννοιες αλληλοσυμπληρούμενες και σε καμία περίπτωση αντίθετες, αποφάνθηκαν το 2007 οι σύνεδροι του United Nations Internet Governance Forum[iv], ενώ οι Ρεπόρτερ Χωρίς Σύνορα διακηρύσσουν ότι, σε μια δημοκρατική και ανοιχτή κοινωνία οι πολίτες είναι εκείνοι που πρέπει να αποφασίσουν σε τι θέλουν να έχουν πρόσβαση και τι θέλουν να βλέπουν στο διαδίκτυο φιλτράρισμα του online περιεχομένου από κυβερνήσεις ή

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

άλλους εξωγενείς μηχανισμούς, είναι ανεπίτρεπτο[v]. Τα όρια ελευθερίας και ιδιωτικότητας τα θέτουν οι χρήστες και μόνο αυτοί.

Οποιαδήποτε συζήτηση για τα δικαιώματα ιδιωτικότητας φτάνει τελικά στο πιο βασικό ερώτημα, δηλαδή "τι σημαίνει προστασία της ιδιωτικής ζωής;" Τι σημαίνει όταν λέμε ότι η συλλογή και η χρήση πληροφοριών από της μηχανές αναζήτησης μπορεί να είναι παρεμβατικές στην ιδιωτική ζωή; Πολλές προσπάθειες έχουν γίνει ώστε να καθοριστούν τα όρια για την προστασία της ιδιωτικής ζωής και πολλοί παραμένουν με την επικείμενη αμφιβολία.[vi]

Για τους σκοπούς της παρούσας έρευνας , αξιοποιήθηκαν ένα από τα υφιστάμενα πλαίσια για την ανάλυση προστασίας της ιδιωτικής ζωής. Η ταξινόμηση του Solove για την Προστασίας Προσωπικών Δεδομένων, δημιουργεί μια ολοκληρωμένη εικόνα σχετικά με το τι εστί ιδιωτικότητα στα πληροφοριακά συστήματα.[vii] Ο Solove βασίζει την ταξινόμηση του "συγκεντρώνοντας πληροφορίες σχετικά με ένα πρόσωπο. "[viii] σχετικά με τις δραστηριότητες που εισβάλλουν στην ιδιωτική ζωή. Αναλύοντας ,τη συλλογή, συγκέντρωση, αποθήκευση, χρήση και την μεταφορά πληροφοριών από τις μηχανές αναζήτησης. Ουσιαστικά αναλύει την πρακτική της συγκέντρωσης πληροφοριών στο πλαίσιο της ιδιωτικής ζωής και των στόχων αναζήτησης ».[ix] Εξηγεί ότι ¨συνδυάζοντας τις πληροφορίες δημιουργούνται συνέργιες. Όταν αναλύονται, συγκεντρωτικές πληροφορίες μπορούν να αποκαλύψουν νέα στοιχεία για ένα άτομο που δεν περίμενε να γίνουν γνωστές γι 'αυτόν, όταν τα αρχικά, μεμονωμένα στοιχεία συλλέχθηκαν.¨ [x]

3.2 Αναφορά στα προσωπικά δεδομένα.

Τα προσωπικά δεδομένα μπορούμε να τα διαχωρίσουμε σε δύο κύριες κατηγορίες στα απλά και τα ευαίσθητα. Τα απλά δεδομένα θεωρούνται πληροφορίες όπως το όνομα το επάγγελμα το μορφωτικό επίπεδο και είναι στοιχεία που αντιστοιχούν το άτομο με την ταυτότητά του με άμεσο ή με έμμεσο τρόπο.

Τη διάκριση αυτή την κατοχυρώνει και ο ν. 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, στο ά. 2 περ. β, όπου τα ευαίσθητα δεδομένα ορίζονται ως :

Τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση

Τα πολιτικά φρονήματα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις.

Η συμμετοχή σε συνδικαλιστική οργάνωση.

Τα δεδομένα για την υγεία.

Η κοινωνική πρόνοια.

Η ερωτική ζωή

Τα σχετικά με ποινικές διώξεις ή καταδίκες.

Και τέλος η συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων Και στο ά. 7 του Νόμου, θεσπίζεται η απαγόρευση επεξεργασίας ευαίσθητων προσωπικών δεδομένων, και αναφέρονται κάποιες εξαιρέσεις.

3.3 Νομοθετικό πλαίσιο εισαγωγή

Στην σύγχρονη εποχή της ελεύθερης διακίνησης της πληροφορίας, τα προσωπικά δεδομένα αποτελούν το σημαντικότερο στοιχείο προάσπισης. Η προστασία και η προάσπιση διαφέρει ανά χώρα και επηρεάζεται σε σημαντικό βαθμό από το πολιτικό και νομικό σύστημα που επικρατούν καθώς και την οικονομική και πολιτιστική πραγματικότητα.

Η παγκοσμιοποίηση και η τεχνολογία είναι δύο έννοιες αλληλένδετες στην σημερινή πραγματικότητα με βασικό συνδετικό κρίκο την ελευθερία διακίνησης ιδεών, αγαθών και υπηρεσιών.

Έτσι κάθε κράτος καλείται να προασπίσει πλέον τα δικαιώματα των πολιτών του με αλλαγές στο νομικό του σύστημα για την προστασία των ελευθεριών, των δικαιωμάτων και της ιδιωτικότητας τους

3.4 Ιστορική αναδρομή στο Ευρωπαϊκό δίκαιο για την ιδωτικότητα

Στην Ευρωπαϊκή ένωση το θέμα της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας είχε δημιουργηθεί νωρίτερα σε σχέση με την Αμερική και επίσης αποφασίστηκε να δημιουργηθεί ένα ποιο συγκεκριμένο και θεσμοθετημένο νομικό πλαίσιο. Έτσι με τη *Σύμβαση της Ρώμης της 4ης Νοεμβρίου 1950,* στο άρθρο 8, δημιουργήθηκε το πρώτο πλαίσιο για την ιδιωτική ζωή των πολιτών.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μετά το συγκεκριμένο άρθρο η Ευρωπαϊκή ένωση θέλησε να δημιουργήσει ένα πλαίσιο το οποίο θα καλύπτει περισσότερες περιπτώσεις και να γίνει ποιο συγκεκριμένο για ποιο ειδικές περιπτώσεις (π.χ. περιπτώσεις τεχνολογικές)

Έτσι με την δημιουργία της Κοινοτικής Οδηγίας 95/46/ΕΚ Η Ευρωπαϊκή ένωση μπορεί πλέον να προασπίσει φυσικά πρόσωπα από την επεξεργασία των προσωπικών δεδομένων τους καθώς και να ελέγχει την κυκλοφορία τους.

Εν συνεχεία και λόγο της αυξανόμενης χρήσης των ηλεκτρονικών επικοινωνιών δημιουργήθηκε μία ακόμα Οδηγία η 97/66/ΕΚ για την διασφάλιση των προσωπικών δεδομένων σε ηλεκτρονικές επικοινωνίες.

Τέλος μία από της ποιο πρόσφατες οδηγίες είναι η 2002/58/ΕΚ η οποία αφορά θέματα όπως οι IP που έχει ένας χρήστης και αποτελούν μια ταυτότητά του.

.

3.5 Περιγραφή της οδηγίας 95/46/ΕΚ76

Η Οδηγία 95/46/ΕΚ76 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, διασφαλίζει την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών[xi].

Με την συγκεκριμένη οδηγία δημιουργείται ένα κανονιστικό πλαίσιο ώστε να υπάρχει από την μία προστασία στην ιδιωτική ζωή των πολιτών και από την άλλη η ελεύθερη κυκλοφορία δεδομένων εντός της ευρωπαϊκής ένωσης. Εντός λοιπόν της οδηγίας οριοθετείτε η χρήση των δεδομένων προσωπικού χαρακτήρα

Η συγκεκριμένη οδηγία δεν εφαρμόζεται σε κάποιες συγκεκριμένες μόνο περιπτώσεις όπως για λόγους εθνική ή δημόσια ασφάλεια, άμυνα κτλ.

Επίσης στην συγκεκριμένη οδηγία γίνεται και ένας προσδιορισμός ως προς την ποιότητα των δεδομένων και την επεξεργασία τους.

Τα δεδομένα ειδικότερα θα πρέπει να έχουν αποκτηθεί μετά από σύμφωνη άποψη του ιδιόκτητη και να έχουν συλλεχτεί για σαφείς και νόμιμους σκοπούς. Επίσης τα δεδομένα αυτά θα πρέπει να επικαιροποιούνται συνεχώς. Τέλος για την επεξεργασία των δεδομένων που έχουν προσωπικό χαρακτήρα θα πρέπει να έχει δοθεί και εδώ η έγκριση του ιδιοκτήτη και είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος ή εμπίπτοντος στην άσκηση δημοσίας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας ή στον τρίτο στον οποίο ανακοινώνονται τα δεδομένα

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Επίσης στο δεύτερο κεφάλαιο της οδηγίας 95/46/ΕC, το άρθρο 6 που έχει σχέση με αρχές της ποιότητας δεδομένων, αναφέρει ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει: γ) να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία, και να διατηρούνται με μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται μόνο κατά τη διάρκεια περιόδου που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών για τους οποίους έχουν συλλέγει ή για τους οποίους αργότερα υφίστανται επεξεργασία. Τα κράτη μέλη προβλέπουν κατάλληλες εγγυήσεις για τα δεδομένα προσωπικού χαρακτήρα που διατηρούνται πέραν της περιόδου αυτής για σκοπούς ιστορικούς, στατιστικούς ή επιστημονικούς.

Το Άρθρο 8 στην συγκεκριμένη οδηγία έχει τεράστια βαρύτητα επειδή αναφέρεται στην επεξεργασία ευαίσθητων προσωπικών δεδομένων Συγκεκριμένα αναφέρει ότι. Τα κράτη μέλη απαγορεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα που παρέχουν πληροφορίες για τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις και την υγεία και τη σεξουαλική ζωή. Βέβαια και εδώ υπάρχει η εξαίρεση η οποία μπορεί να άρει την συγκεκριμένη απαγόρευση και η οποία δεν ισχύει όταν :

α) το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει ρητά τη συγκατάθεσή του για την επεξεργασία, εκτός αν η νομοθεσία του κράτους μέλους ορίζει ότι η συγκατάθεση δεν αίρει την απαγόρευση της παραγράφου 1. Αυτό δηλαδή φανερώνει ότι στην Ευρωπαϊκή νομοθεσία είναι ότι η συγκατάθεση ενός ανθρώπου είναι πολύ σημαντική σχετικά με το εάν έχει προστασία ή όχι.

Ένα πολύ σημαντικό άρθρο, της ίδιας οδηγίας, σχετικά με το θέμα είναι και το Άρθρο 11, που αναφέρεται στις περιπτώσεις στις οποίες Όταν τα δεδομένα δεν έχουν συλλεχτεί από το πρόσωπο το οποίο αφορούν, τα κράτη μέλη προβλέπουν ότι, ευθύς ως καταχωρηθούν τα δεδομένα ή, εάν προβλέπεται ανακοίνωσή τους σε τρίτους, το αργότερο κατά την πρώτη ανακοίνωσή τους, ο υπεύθυνος της επεξεργασίας ή ο εκπρόσωπός του πρέπει να παρέχει στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα τις εξής πληροφορίες, εκτός εάν το πρόσωπο αυτό έχει ήδη ενημερωθεί: α) την ταυτότητα του υπευθύνου της επεξεργασίας και, ενδεχομένως, του εκπροσώπου του β) τους σκοπούς της επεξεργασίας γ)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

οποιαδήποτε περαιτέρω πληροφορία, όπως: τις κατηγορίες των σχετικών δεδομένων, τους αποδέκτες ή τις κατηγορίες αποδεκτών, την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα που το αφορούν και δικαιώματος διόρθωσής τους, εφόσον οι πληροφορίες αυτές είναι αναγκαίες, λόγω των ειδικών συνθηκών υπό τις οποίες συλλέγονται τα δεδομένα, ώστε να εξασφαλίζεται θεμιτή επεξεργασία, έναντι του προσώπου στο οποίο αναφέρονται τα δεδομένα.

Επίσης ειδική αναφορά γίνεται για τα δικαιώματα που πρέπει να έχουν όσοι είναι οι ιδιοκτήτες των δεδομένων. Έτσι μπορούν να απαιτήσουν διαβεβαιώσεις εάν τα δεδομένα τους θα δημοσιευτούν ή επεξεργαστούν από τους υπεύθυνους επεξεργασίας. Επίσης εάν δεν συμφωνούν με οποιασδήποτε επεξεργασία μπορούν να απαιτήσουν την διαγραφή των δεδομένων τους. Επίσης ο υπεύθυνος επεξεργασίας θεωρείτε υπεύθυνος σε περίπτωση που τα αρχεία αλλοιωθούν ή σε περίπτωση απώλειας τους.

Σε αντίθετες περιπτώσεις ο ιδιοκτήτης θα πρέπει να του δίνετε η δυνατότητα να καταφύγει σε νομικές λύσεις. Μάλιστα εάν έχει θιχτεί σε οποιοσδήποτε επίπεδο θα πρέπει να αποδοθούν ποινές στους υπεύθυνους αλλά και αποζημιώσεις στον ιδιοκτήτη των δεδομένων.

Τέλος υπάρχουν κάποιοι περιορισμοί στην πρόσβαση και την επεξεργασία των δεδομένων από τον ιδιοκτήτη για περιπτώσεις που αφορούν θέματα εθνικής ασφάλειας.

Για την μεταβίβαση των δεδομένων προς τρίτες χώρες μόνο εάν υπάρχει το κατάλληλο νομοθετικό πλαίσιο το οποίο θα αναφερθεί στην ανάλυση των νομοθεσιών εκτός Ευρωπαϊκής ένωσης.

Σε εθνικό επίπεδο οι κοινοτικές οδηγίες έχουν προσαρμοστεί στο νομοθετικό τους πλαίσιο. Έτσι γίνεται και στην Ελλάδα. Η επιτήρηση και ο έλεγχος γίνεται από ανεξάρτητες αρχές.

3.6 Ομάδα εργασίας του άρθρο 29

Ειδική αναφορά πρέπει να γίνει και στην ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα , ή αλλιώς ομάδα του Άρθρου 29 [xii]. Η σύσταση της αναφέρετε στο άρθρου 29 της οδηγίας 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η ομάδα έχει συμβουλευτικό χαρακτήρα ως προς την Ευρωπαϊκή επιτροπή αλλά είναι ανεξάρτητη ως προς αυτήν. Απαρτίζεται από έναν εκπρόσωπο των Αρχών Προστασίας Δεδομένων κάθε κράτους μέλους και εξετάζει θέματα ιδιαίτερης βαρύτητας ή θέματα που παρουσιάζουν ειδικότερο ενδιαφέρον σχετικά με την προστασία των προσωπικών δεδομένων και εμπίπτουν στον πρώτο πυλώνα της ΕΕ. Η εξέταση των θεμάτων γίνεται είτε μετά από αίτηση της Ευρωπαϊκής επιτροπής είτε με πρόταση των μελών της ομάδας. Η ομάδα εκδίδει γνωμοδοτήσεις και κείμενα εργασίας.

Ο σκοπός της ομάδας αποτελείται από τέσσερις συνιστώσες:

(α) να εξετάζει οποιοδήποτε θέμα σχετικό με την εφαρμογή των εθνικών διατάξεων που έχουν θεσπισθεί κατ' εφαρμογή της εν λόγω οδηγίας, ώστε να συμβάλλει στην ομοιόμορφη εφαρμογή τους,

(β) να παρέχει στην Επιτροπή τη γνώμη της σχετικά με το επίπεδο προστασίας στην Κοινότητα και στις τρίτες χώρες,

(γ) να συμβουλεύει την Επιτροπή για κάθε σχέδιο τροποποιήσεως της εν λόγω οδηγίας, κάθε σχέδιο συμπληρωματικών ή ειδικών μέτρων που πρέπει να ληφθούν για τη διασφάλιση των δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, καθώς και για κάθε άλλο σχέδιο κοινοτικών μέτρων που έχουν επιπτώσεις επί αυτών των δικαιωμάτων και ελευθεριών, και

(δ) να γνωμοδοτεί επί των κωδίκων δεοντολογίας που εκπονούνται σε κοινοτικό επίπεδο.

3.7 Ελληνική Νομοθεσία

Στην Ελλάδα η κοινοτική οδηγία έχει ενσωματωθεί από πολύ νωρίς. Συγκεκριμένα για τα προσωπικά δεδομένα υπάρχει ο νόμος 2472/1997 [xiii] ο οποίος ορίζει σαν εποπτική αρχή την αρχή προστασίας δεδομένων.

Στον νόμο αυτό αρχικά ορίζονται τι είναι προσωπικά αλλά και τι είναι ευαίσθητα προσωπικά δεδομένα τα οποία έχουν αναφερθεί και παραπάνω. Άλλη μία έννοια είναι

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

το υποκείμενο των δεδομένων το οποίο είναι το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα. Εν συνεχεία αναλύονται έννοιες όπως Επεξεργασία δεδομένων προσωπικού χαρακτήρα, Αρχείο δεδομένων προσωπικού χαρακτήρα, Εκτελών την επεξεργασία, τρίτος, αποδέκτης, Υπεύθυνος επεξεργασίας δεδομένων.

Ειδική αναφορά γίνεται και στον τρόπο επεξεργασίας των δεδομένων. Αρχικά τα δεδομένα θα πρέπει να έχουν συλλεχθεί με νόμιμο τρόπο, για συγκεκριμένο χρόνο, να είναι ακριβή και όχι περισσότερα από τα απαραίτητα.

Η βασική προϋπόθεση για να γίνει οποιασδήποτε επεξεργασία είναι να έχει δώσει το υποκείμενο την συγκατάθεσή του. Βέβαια υπάρχουν και εξαιρέσεις. Επίσης ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώνει την ανεξάρτητη αρχή για κάθε τυχόν αλλαγή που θα κάνει. Επίσης ο συγκεκριμένος νόμος αναφέρετε και στα ευαίσθητα προσωπικά δεδομένα τα οποία δεν μπορούν να επεξεργαστούν εκτός κάποιων εξαιρέσεων

Πολύ σημαντικό κομμάτι είναι και η διασύνδεση των δεδομένων στο άρθρο 8 η οποία απαιτεί την γνώση αλλά και την έγκριση της αρχής. Επίσης η κίνηση των αρχείων εκτός Ευρωπαϊκής ένωσης πρέπει να γίνεται κάτω από ορισμένες προϋποθέσεις όπως να υπάρχει ανάλογο επίπεδο ασφαλείας με της χώρας μας ή γίνεται με την άδεια της αρχής όταν συντρέχουν κάποιοι ιδιαίτεροι λόγοι.

Επίσης αναφέρονται και τα δικαιώματα του χρήστη τα οποία είναι τα:

Δικαίωμα ενημέρωσης.

Δικαίωμα πρόσβασης.

Δικαίωμα αντίρρησης.

Δικαίωμα προσωρινής δικαστικής προστασίας.

Στο τέλος αναφέρει και την σύνθεση της εποπτικής αρχής που όπως αναφέρθηκε και παραπάνω είναι η αρχή προστασίας δεδομένων. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), ή αλλιώς και Αρχή Προστασίας Προσωπικών Δεδομένων, είναι συνταγματικά κατοχυρωμένη από το σύνταγμα σαν ανεξάρτητη διοικητική Αρχή. Ιδρύθηκε βάση του νόμου 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος ενσωματώθηκε στο

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ελληνικό δίκαιο ύστερα από την ευρωπαϊκή οδηγία 95/46/ΕΚ. Η οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης. Η Αρχής ξεκίνησε την λειτουργία στις 10 Νοεμβρίου 1997.

Η συγκεκριμένη αρχή λειτουργεί με γνώμονα τον σεβασμό και την προστασία της αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας τα οποία αποτελούν θεμελιώδη και πρωταρχική επιδίωξη κάθε δημοκρατικής κοινωνίας.

Για να γίνετε καλύτερος και ποιο ακριβής ο έλεγχος της επεξεργασίας δεδομένων η αρχή διατηρεί και τα ακόλουθα μητρώα [xiv]:

Μητρώο Αρχείων και Επεξεργασιών, στο οποίο περιλαμβάνονται τα αρχεία και οι επεξεργασίες που γνωστοποιούνται στην Αρχή.

Μητρώο Αδειών, στο οποίο περιλαμβάνονται οι άδειες που εκδίδει η Αρχή για την ίδρυση και λειτουργία αρχείων που περιέχουν ευαίσθητα δεδομένα.

Μητρώο Διασυνδέσεων, στο οποίο περιλαμβάνονται οι δηλώσεις και οι άδειες που εκδίδει η Αρχή για τη διασύνδεση αρχείων.

Μητρώο προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία, τα οποία έχουν ως σκοπό την προώθηση προμήθειας αγαθών ή την παροχή υπηρεσιών εξ αποστάσεως.

Μητρώο Αδειών Διαβίβασης, στο οποίο καταχωρίζονται οι άδειες διαβίβασης δεδομένων προσωπικού χαρακτήρα.

Μητρώο Απόρρητων Αρχείων, στο οποίο καταχωρίζονται, με απόφαση της Αρχής ύστερα από αίτηση του εκάστοτε υπεύθυνου επεξεργασίας, αρχεία που τηρούν τα Υπουργεία Εθνικής Άμυνας και Δημόσιας Τάξης καθώς και η Εθνική Υπηρεσία Πληροφοριών, για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Στο Μητρώο Απόρρητων Αρχείων καταχωρίζονται και οι διασυνδέσεις με ένα τουλάχιστον αρχείο της περίπτωσης αυτής.

Επίσης άλλες αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων είναι στην Ελλάδα η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και στην Ευρώπη ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.8 Αναδρομή στην δημιουργία νομικού πλαισίου περί της ιδιωτικότητας στις ΗΠΑ

Προκειμένου να αναλύσουμε την κατάσταση της ανάγκης για νομική προστασία των χρηστών του διαδικτύου, πρέπει πρώτα να καταλάβουμε λίγο πιο πολύ το νομικό πλαίσιο που υπάρχει τώρα. Στην Αμερική, σχετικά με την ιδωτικότητα, υπάρχουν τρεις σημαντικές υποθέσεις, δυο από τις οποίες έγιναν τη δεκαετία των εβδομήντα – η *US vs. Miller (1976)* και η *Smith vs. Maryland(1979)*. Πριν από αυτές υπήρχε και η US vs. Katz (1967), μια υπόθεση που θεωρείται αρκετά σημαντική για το θέμα, στην οποία ο δικαστής δημιούργησε ένα πλαίσιο για να καθοριστεί εάν κάποιος έχει «λογικές προσδοκίες ιδιωτικότητας». Δηλαδή, ένα πλαίσιο που καθορίζει εάν κάποιος μπορεί να περιμένει συνταγματική προστασία όταν νιώθει ότι τα δικαιώματά του έχουν παραβιαστεί σχετικά με την ιδωτικότητα. Αυτά τα δικαιώματα προστατεύονται από την τέταρτη τροπολογία του Αμερικάνικου Συντάγματος. Το προαναφερθέν πλαίσιο λέει ότι ένας άνθρωπος μπορεί να απαιτήσει προστασία από το νόμο εάν έχει επιδείξει μια υποκειμενική προσδοκία για ιδωτικότητα, και εάν αυτή η προσδοκία είναι μια την οποία η κοινωνία θα δεχόταν ως λογική. Μετά όμως, στην υπόθεση *US vs. Miller*, το Ανώτατο Δικαστήριο αποφάνθηκε ότι οι πελάτες των τραπεζών δεν μπορούν να έχουν ως απαίτηση το προσωπικό απόρρητο, σχετικά με τα δεδομένα που έχουν δώσει οι ίδιοι στην τράπεζα. Εάν κάποιος παραδώσει εθελοντικά κάποια δεδομένα, αποφάνθηκε το ΑΔ, δεν μπορεί να έχει ως προσδοκία ότι το τρίτο πρόσωπο (σε αυτή την περίπτωση, η τράπεζα, αλλά ισχύει και για μηχανές αναζήτησης) δεν θα παραδώσει τα δεδομένα στην κυβέρνηση.

Βέβαια, αυτή η απόφαση είναι πολύ σημαντική για την προστασία των προσωπικών δεδομένων – και αυτό που αποφάνθηκε το ΑΔ στην υπόθεση *Smith vs. Maryland* έχει ακόμα πιο ανησυχητικές επιπτώσεις. Υπό παρόμοιες συνθήκες, το ΑΔ αποφάνθηκε ότι δεν μπορεί κάποιος να έχει την προαναφερθείσα προσδοκία για τους αριθμούς τηλεφώνων που καλεί – δηλαδή ότι δεν έχει το δικαίωμα να περιμένει νομική προστασία της ιδιωτικότητάς του από τη στιγμή που έχει παραδώσει τις πληροφορίες εθελοντικά σε τρίτο πρόσωπο, κάτι που, θεωρητικά, κάνει όταν καλεί έναν αριθμό μέσω ενός τηλεφωνικού κέντρου[xv].

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.9 Νομικό πλαίσιο των ΗΠΑ στο οποίο υπόκεινται εταιρείες μηχανών αναζήτησης

Ένα γενικότερο πλαίσιο για την παραγωγή πολιτικών ιδιωτικότητας που υπάρχει είναι αυτό που έχει προσδιοριστεί στα πλαίσια ΗΠΑ-ΕΕ και ΗΠΑ-Ελβετικά "Safe Harbor". Αυτά τα δυο φτιάχτηκαν από την Αμερικανική κυβέρνηση, ως κατευθυντήριο γραμμών όσον αφορά την προστασία δεδομένων. Ωστόσο, δεν είναι νομοθεσία, και ως εκ τούτου δεν υποχρεούνται οι εταιρείες και ειδικά οι μηχανές αναζήτησης να ακολουθούν τις προτάσεις τους. Λειτουργεί όμως όπως κάποια από τα πρότυπα ISO – καθώς δεν υποχρεωτικά, παρόλα αυτά, πολλές εταιρείες τα χρησιμοποιούν ως ετικέτα για διαφήμιση κτλ. όπως η Google.

3.10 Τα αίτια δημιουργίας του safe Harbor

Τα πλαίσια αυτά δημιουργήθηκαν προκειμένου να αντιμετωπίσουν τις διαφορές μεταξύ των πολιτικών που χρησιμοποιούν οι Ευρωπαϊκή Ένωση και οι ΗΠΑ. [xvi] Το 1998, η Ευρωπαϊκή Ένωση άλλαξε την πολιτική της για να απαγορεύσει την μεταφορά δεδομένων από Ευρωπαϊκές χώρες σε χώρες εκτός της Ένωσης που δεν έχουν κατάλληλη νομοθεσία ανάλογα με το Ευρωπαϊκό πρότυπο για την προστασία δεδομένων. Λόγω αυτού, φτιάχτηκε το «Safe Harbor» πλαίσιο. Το πλαίσιο αυτό αποτελεί έναν τρόπο συμμόρφωσης Αμερικάνικων οργανισμών με την Ευρωπαϊκή νομοθεσία για να διευκολύνει τις διεθνές ηλεκτρονικές ανταλλαγές. Από αυτό μπορούμε να καταλάβουμε ότι τα κενά που υπάρχουν στην Αμερικάνικη νομοθεσία θεωρητικά καλύπτονται από ιδιωτικές πολιτικές ιδιωτικότητας που έχουν οι μηχανές αναζήτησης – και προφανώς είτε πιστεύει η Αμερικανική κυβέρνηση ότι αυτό το πλαίσιο επαρκεί (η ύπαρξη του πλαισίου είναι αποδεικτικό ότι η νομοθεσία που καλύπτει τα ίδια θέματα δεν χρειάζεται), είτε δεν είναι πιθανό πολιτικά να δημιουργήσουν νομοθεσία να υποχρεώσει τις Αμερικανικές εταιρείες να έχουν πολιτικές που είναι τουλάχιστον όμοιες με την πολιτική που προτείνεται από το πλαίσιο «Safe Harbour».

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Το πλαίσιο αυτό περιέχει κάποιες αρχές σχετικά με το πως θα χρησιμοποιούνται οι πληροφορίες που κρατάει οποιαδήποτε εταιρεία. Η ιστοσελίδα του «Safe Harbor» [xvii]πλαισίου αναφέρει για τις προειδοποιήσεις που πρέπει να έχει οποιαδήποτε εταιρεία που συμμετέχει στο πρόγραμμα. Η αναφορά γίνεται ως εξής – «Ένας οργανισμός οφείλει να ενημερώσει τα άτομα σχετικά με τους σκοπούς για τους οποίους συλλέγει και χρησιμοποιεί πληροφορίες που τα αφορούν, τον τρόπο επικοινωνίας με τον οργανισμό με όλα τα ερωτήματα ή παράπονα, τους τύπους των τρίτων στους οποίους γνωστοποιεί τις πληροφορίες, τις επιλογές και σημαίνει ότι η οργάνωση προσφέρει στα άτομα για τον περιορισμό της χρήσης και της γνωστοποίησης. Η παρούσα ανακοίνωση πρέπει να παρέχεται σε σαφή και κατανοητή γλώσσα και να παρέχει προσωπικές πληροφορίες για τον οργανισμό ή το συντομότερο μετά από αυτή όσο είναι εφικτό, αλλά σε κάθε περίπτωση πριν από την οργάνωση χρησιμοποιεί τα στοιχεία αυτά για σκοπό διάφορο εκείνου για τον οποίο ήταν αρχικά συλλογή ή επεξεργασία από τον οργανισμό ή τη μεταφορά αποκαλύπτει για πρώτη φορά σε ένα τρίτο μέρος .

Εν συνεχεία παρέχει αρχές για τις επιλογές των χρηστών οι οποίες αφορούν τα δεδομένα πάνω στα οποία πρέπει θεωρητικά να έχει μια επιλογή ο χρήστης ή να μπορεί να τα διαμορφώνει μέχρι ένα συγκεκριμένο επίπεδο. Συνεχίζει λοιπόν η ιστοσελίδα ως εξής: «Ένας οργανισμός πρέπει να προσφέρει στα άτομα την ευκαιρία να επιλέγουν (opt out) [δηλαδή, εάν δεν επιλέγει ενεργητικά ο χρήστης ότι δεν θα δοθούν, τα δεδομένα μπορούν να δοθούν σε τρίτο πρόσωπο] εάν τα προσωπικά τους στοιχεία είναι να γνωστοποιηθούν σε ένα τρίτο πρόσωπο ή να χρησιμοποιηθούν για ένα σκοπό που δεν συμβιβάζεται με το σκοπό για τους οποίους συλλέχθηκαν αρχικά ή μεταγενέστερα εξουσιοδοτήθηκαν από το άτομο. Τα άτομα πρέπει να παρέχονται με σαφούς και εμφανείς, άμεσα διαθέσιμους και οικονομικά προσιτούς μηχανισμούς να ασκούν επιλογή.» Συνεχίζει και εξηγεί ότι πρέπει σχετικά με ευαίσθητες πληροφορίες μια εταιρεία που συμμετέχει στο πρόγραμμα να πρέπει να επιλέγει ενεργητικά ο χρήστης ότι μπορούν να δοθούν σε τρίτο πρόσωπο για να μπορεί η εταιρεία να το κάνει ή να χρησιμοποιήσει τα δεδομένα για σκοπό διαφορετικό από αυτό για τον οποίο είχαν συλλεχθεί.

Η τρίτη αρχή έχει σχέση με την παράδοση πληροφοριών σε τρίτα πρόσωπα. Εδώ η εταιρεία στο πρόγραμμα πρέπει να προσέχει μόνο ότι ακολουθεί τις πρώτες δύο αρχές, και να σιγουρεύεται ότι οποιοδήποτε τρίτο πρόσωπο στο οποίο θα δώσει

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πληροφορίες ακολουθεί τις ίδιες αρχές. Πουθενά όμως δεν αναφέρει ότι πρέπει να ενημερωθεί ο άνθρωπος τον οποίον αφοράνε οι πληροφορίες σε ποιους οργανισμούς ή ανθρώπους δίνονται οι πληροφορίες, το οποίο είναι υποχρεωτικό στην Ευρωπαϊκή Ένωση όπως αναφέρουμε παρακάτω.

Επιπλέον το πλαίσιο έχει αρχές για ασφάλεια, ακεραιότητα δεδομένων, πρόσβαση και επιβολή (των αρχών). Για την ασφάλεια, πρέπει κάθε εταιρεία πρέπει να προβεί σε εύλογες προφυλάξεις – στο πώς ακριβώς καθορίζεται το εάν είναι εύλογες ή όχι δυστυχώς δεν αναφέρεται το κείμενο. Πέρα από αυτό λέει ότι οι άνθρωποι στους οποίους αφορούν οι πληροφορίες πρέπει να έχουν πρόσβαση στα δεδομένα προκειμένου να μπορούν να αλλάζουν ή να διαγράψουν πληροφορίες που δεν είναι σωστές.

4. Ιδιωτικότητα και μηχανές αναζήτησης

Για το θέμα της ιδιωτικότητας, σχετικά με τις μηχανές αναζήτησης, υπάρχουν δύο σημαντικά ερωτήματα που πρέπει να αναλυθούν. Το ένα έχει σχέση με το γεγονός ότι οι μηχανές αναζήτησης κρατάνε πολλές πληροφορίες για τους χρήστες τους – και το άλλο έχει ως θέμα τις πιθανότητες για έναν χρήστη να βρίσκει πολλές πληροφορίες για κάτι ή για κάποιον γρήγορα, εύκολα, και από πολλές διαφορετικές πηγές. Βάση αυτών, υπάρχει μέσω των μηχανών αναζήτησης η ικανότητα να δημιουργήσει κάποιος μια λεπτομερή λίστα πληροφοριών για ένα συγκεκριμένο πρόσωπο.

Όσον αφορά στην αντιμετώπιση των διάφορων νομικών θεσμών, είτε εθνικών, είτε διεθνών, είναι ξεκάθαρο ότι δεν ευθύνονται οι μηχανές αναζήτησης για τις πληροφορίες που μεταφέρουν σε οποιονδήποτε χρήστη. Ούτε αυτοί που παρέχουν τις πληροφορίες ευθύνονται νομικά – γενικώς, δεν θεωρείται έγκλημα η πράξη του να παρέχει κάποιος ιδιωτικές πληροφορίες, εκτός από συγκεκριμένες περιπτώσεις και συγκεκριμένα θέματα.

Πέρα από αυτό, προφανώς ευθύνεται και το άτομο το οποίο αφορούν οι πληροφορίες. Καθώς κάποιος μπορεί να δίνει αναληθές πληροφορίες για κάποιον, πραγματικές πληροφορίες θα υπάρχουν στο διαδίκτυο μόνο εάν το άτομο το οποίο αφορούν τις παράγει σε κάποια διαδικτυακή υπηρεσία. Από τα παραπάνω γίνεται κατανοητό ότι ο οποιοσδήποτε χρήστης φέρει την ευθύνη ακόμα και όταν έχει δώσει τη συγκατάθεσή του. Το πρόβλημα που φανερώνεται και αντιμετωπίζουν οι διάφοροι νομικοί θεσμοί είναι ότι κάποιος μπορεί με μεθοδική και στοχευόμενη προσπάθεια να συγκεντρώσει αρκετές πληροφορίες που αφορούν κάποιο πρόσωπο και υπάρχουν στο διαδίκτυο.

4.1 Τι δεδομένα <<συλλέγει >> μια μηχανή αναζήτησης κάθε φορά που επιλέγει να κάνει ο χρήστης μια αναζήτηση και τι επιπτώσεις έχει αυτό.

Οι μηχανές αναζήτησης έχουν γίνει μέρος της καθημερινότητας των χρηστών του διαδικτύου και αποτελούν ένα βασικό εργαλείο αναζήτησης και ανάκτησης πληροφορίας . Έχουν τη δυνατότητα να παρακολουθούν αναζητήσεις ενός χρήστη. Οι προσωπικές πληροφορίες μπορούν να αποκαλυφθούν μέσω των αναζητήσεών τους,

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συμπεριλαμβανομένων των όρων που χρησιμοποιήθηκαν στην αναζήτηση, τη στιγμή της αναζήτησης, και πολλά άλλα. Οι μηχανές αναζήτησης έχουν υποστηρίξει μια αναγκαιότητα για να διατηρούν τις πληροφορίες αυτές προκειμένου να παρέχουν καλύτερες υπηρεσίες, για την προστασία υπό πίεση της ιδιωτικότητας, και την προστασία κατά της απάτης. [1] Μια μηχανή αναζήτησης παίρνει όλους τους χρήστες της και εκχωρεί σε κάθε έναν συγκεκριμένο αριθμό ταυτότητας. Στη βάση δεδομένων συχνά διατηρούνται αρχεία περιήγησης στο Διαδίκτυο του κάθε μέλους.

Οι μηχανές αναζήτησης είναι επίσης σε θέση να διατηρούν πληροφορίες για το χρήστη, την τοποθεσία και τον χρόνο από την χρονική στιγμή που χρησιμοποιήθηκε η μηχανή αναζήτησης μέχρι και ενενήντα ημέρες. Τα περισσότερα από τα δεδομένα που διατηρούνται από τους φορείς εκμετάλλευσης από τις μηχανές αναζήτησης χρησιμοποιούν τα δεδομένα για να πάρουν μια προδιάθεση για κυρίως στατιστικά ερωτήματα που πρέπει να απαντηθούν ανά περιοχές οι τομείς. Επίσης οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για έρευνα και τον δικαστικό τομέα σε ορισμένες περιπτώσεις.

Και αν αυτό είναι εμφανές μετά από λίγες αναζητήσεις, θα πρέπει να γίνει αναφορά και για το μέγεθος και το βάθος των πληροφοριών που συλλέγονται σε ένα αρχείο καταγραφής αναζήτησης που περιέχουν χιλιάδες και χιλιάδες αναζητήσεις για μια περίοδο μηνών ή ετών. Ελάχιστοι είναι οι χρήστες που έχουν επίγνωση των πρακτικών συλλογής δεδομένων των μηχανών αναζήτησης «πιθανώς υποτιμούν τον αντίκτυπο και την παρεμβατικότητα στην ιδιωτική ζωή τους, καθιστώντας την με την πάροδο του χρόνου "διαφανή"».[xviii]Αυτό που περιπλέκει τα πράγματα ακόμα περισσότερο είναι η μεγάλη συγκέντρωση του κλάδου των μηχανών αναζήτησης.
Παρά τη μεγάλη τους χρησιμότητα, υπάρχουν ζητήματα σχετικά με τον μεγάλο όγκο των προσωπικών δεδομένων που διατηρούν, κυρίως μέσω των αρχείων καταγραφής των αναζητήσεων (search logs), που πραγματοποιούν οι χρήστες. Τα αρχεία αυτά περιέχουν αρκετή πληροφορία, που μπορεί τελικά να οδηγήσει ακόμα και στην αναγνώριση του χρήστη, όπως π.χ. το ίδιο το ερώτημα της αναζήτησης, την IP διεύθυνση του χρήστη, την ώρα και μέρα της αναζήτησης, το λειτουργικό σύστημα του υπολογιστή του χρήστη, τη γλώσσα που χρησιμοποιήθηκε, τα cookies ή άλλα

[1] Online Privacy:χρησιμοποιόντας το ιντερνετ με ασφάλεια για περισσοτερες πληροφορίες στο άθρο: fromhttp://www.privacyrights.org/fs/fs18-cyb.htm

συναφή προγράμματα που έχουν εγκατασταθεί στον υπολογιστή του χρήστη, κ.ά. Πολύ συχνά η πληροφορία αυτή χρησιμοποιείται από τις ίδιες τις μηχανές αναζήτησης για να προσφέρουν στοχευμένη διαφήμιση στο χρήστη, ανάλογα με τις προτιμήσεις που ο ίδιος φαίνεται να έχει βάσει των αναζητήσεων που πραγματοποιεί. Οι βάσεις δεδομένων των μηχανών αναζήτησης, στην ουσία δημιουργούν προφίλ των χρηστών, τα οποία μπορούν να επηρεάσουν την ιδιωτική και κοινωνική ζωή τους, ειδικά στις περιπτώσεις που τα δεδομένα των αναζητήσεων είναι ελλιπή, λανθασμένα ή υπερβολικά.

Το «cookie» είναι ένα μικρό αρχείο με πληροφορίες που μια ιστοσελίδα (συγκεκριμένα ο διακομιστής ιστού - web server) αποθηκεύει στον υπολογιστή ενός χρήστη, ώστε να μπορεί αργότερα να έχει πρόσβαση σε αυτές τις πληροφορίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα. Ο διαχειριστής μιας ιστοσελίδας μπορεί να εγκαταστήσει ένα «cookie» που δεν είναι απαραίτητο για τη βασική λειτουργία μιας ιστοσελίδας, μόνο εάν ο εκάστοτε χρήστης της ιστοσελίδας έχει δώσει τη συγκατάθεσή του μετά από σαφή και εκτενή ενημέρωση για την εγκατάσταση αυτή, το σκοπό της επεξεργασίας, την άσκηση του δικαιώματος πρόσβασης και τυχόν αποδέκτες των δεδομένων. Για τα cookies που είναι απαραίτητα για τη λειτουργία της ιστοσελίδας και την παροχή υπηρεσιών, που ζητάει ο χρήστης της, απαιτείται ενημέρωση και η παροχή δυνατότητας άρνησης εγκατάστασής τους.

Επίσης πολλές από τις ιστοσελίδες που επισκεπτόμαστε, φυλάνε στον υπολογιστή μας δεδομένα για την επίσκεψη μας, τα λεγόμενα “Cookies”. Τα Cookies είναι μικρά κομμάτια από πληροφορίες όπως το όνομα χρήστη, πληροφορίες της εγγραφής μας σε μια σελίδα, προτιμήσεις, διαδικτυακά «καλάθια με ψώνια» και λοιπά. Οι νόμιμες εταιρείες χρησιμοποιούν τα Cookies για να κάνουν προσφορές σε χρήστες που τους επισκέπτονται ξανά. Παράνομες εταιρείες χρησιμοποιούν Cookies για να πάρουν πληροφορίες για τους χρήστες και να τις πουλήσουν σε εταιρείες Marketing.

Προσοχή χρειάζεται και όταν γίνεται αποστολή Μηνυμάτων της Στιγμής (Instant Messages) π.χ. με Google Talk ή με Microsoft Live Messenger. Πρέπει να γνωρίζουμε ότι πολλές από αυτές τις εταιρείες αυτόματα αποθηκεύουν τα μηνύματά μας, εκτός και εάν έχουμε κάνει τις ανάλογες ρυθμίσεις.

Η ολοκληρωμένη και λεπτομερή ταξινόμηση του Solove της ιδιωτικότητας και των τρόπων παραβίασης της κατονομάζει τους παρακάτω παράγοντες και την προστασία της ιδιωτικής ζωής, οι οποίες παραβιάζονται κυρίως από τη συλλογή, τη διατήρηση και την χρήση από τις μηχανές αναζήτησης των κορμών αναζήτησης. Οι δραστηριότητες της κάθε μηχανής αναζήτησης θέτουν το πρόβλημα της συγκέντρωσης, επειδή οι προσωπικές πληροφορίες και τα ολοκληρωμένα προφίλ ενός χρήστη συλλέγονται από τα κομμάτια των πληροφοριών που αποκαλύπτει με την πάροδο του χρόνου. Της παραμόρφωσης πληροφοριών, επειδή οι πληροφορίες στα αρχεία καταγραφής αναζήτησης μπορεί να είναι άκρως παραπλανητικές με δυνητικά σκληρά αποτελέσματα για τους χρήστες. Του αποκλεισμού, επειδή οι χρήστες δεν έχουν πρόσβαση στα αρχεία τους. Τέλος της Δευτερεύουσας χρήσης, επειδή η μηχανή αναζήτησης χρησιμοποιεί δεδομένα που συλλέγονται από τους χρήστες για ένα σκοπό (την έρευνα) με διαφορετικούς σκοπούς από την μηχανή αναζήτησης (εμπορικούς, την ασφάλεια, την επιβολή του νόμου, την άσκηση προσφυγής), και παραβίασης του απορρήτου. Επειδή η κάθε μηχανή αναζήτησης έχει το καθήκον της εμπιστευτικότητας με βάση ένα σιωπηρό όρο της σύμβασης και της ιδιωτικής φύσης της ίδιας της πληροφορίας. Πρόσθετα προβλήματα ασφάλειας της ιδιωτικής ζωής, όπως η αποκάλυψη, η επιτήρηση, η ανασφάλεια και η αποκάλυψη εν συντομία, καθώς και το μούδιασμα ότι οι πρακτικές απορρήτου της κάθε μηχανής αναζήτησης θα μπορούσαν να έχουν σοβαρές επιπτώσεις στον χρήστη.

4.2 Η χρήση των πληροφοριών από τρίτα πρόσωπα

Η ιδιωτικότητα του χρήστη έχει μια μεγάλη διαφορά ως προς την ιδιωτικότητα ενός τρίτου προσώπου – ο χρήστης από τη μία έχει μια σχέση εμπιστοσύνης με μια μηχανή αναζήτησης, ενώ το τρίτο πρόσωπο όχι. Για τη μηχανή αναζήτησης, ή τουλάχιστον για την εταιρεία που διαχειρίζεται μια μηχανή αναζήτησης, υπάρχει ο πειρασμός ότι μπορούν να πουλήσουν ή να χρησιμοποιήσουν κάποιες ιδιωτικές πληροφορίες για εμπορικούς σκοπούς. Τα τρίτα πρόσωπα δεν έχουν το ίδιο πρόβλημα, αλλά μπορούν πιο εύκολα να γίνουν στόχοι καταδίωξης.

Το γεγονός ότι οι μηχανές αναζήτησης κρατάνε πολλές πληροφορίες για τους χρήστες τους είναι δυστυχώς απαραίτητο για την αποτελεσματική παραγωγή χρήσιμων

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αποτελεσμάτων μιας ηλεκτρονικής αναζήτησης. Όταν ένας χρήστης αναζητεί κάτι, η πράξη αυτή καθαυτή δίνει πληροφορίες για το τι τον ενδιαφέρει, και τι θέλει να μάθει. Γίνεται λοιπόν ξεκάθαρο, ότι μέσω πολλών και διαφορετικών αναζητήσεων, φανερώνεται ένα κομμάτι της προσωπικότητάς του (προτιμήσεις, γνώσεις, επιθυμίες, κτλ.) και αυτές οι πληροφορίες αποτελούν μια πηγή δεδομένων που μπορεί μεν να χρησιμοποιηθεί προκειμένου να του προσφερθούν ανάλογες διαφημίσεις σχετικά με τα ενδιαφέροντά του, ή αλλιώς να χρησιμοποιηθεί ώστε να βρει κάποιος πολλές πληροφορίες για έναν άνθρωπο. Βέβαια, πλέον, με τον όγκο των ηλεκτρονικών αναζητήσεων παγκοσμίως, οι μηχανές αναζήτησης έχουν μαζέψει ένα τεράστιο ποσό δεδομένων για τους χρήστες τους.

4.3 Οι πληροφορίες που συλλέγονται πως χρησιμοποιούνται και τι επιπτώσεις έχουν.

Στην εποχή του Web 2.0, έχει δημιουργηθεί ένα δίκτυο ανταλλαγής απόψεων, μία επικοινωνιακή πλατφόρμα με υλικό που παράγεται και προωθείται από τους ίδιους τους χρήστες. Πρόκειται για ένα ιδιαίτερα «αυτορυθμισμένο» σύστημα διαδραστικής επικοινωνίας, οπού τα όρια ασφάλειας και ελευθερίας του καθενός ουσιαστικά καθορίζονται από την προσωπικότητα του ίδιου του χρήστη.

Ο λόγος που κάποιος ανεβάζει φωτογραφίες στο facebook, χιουμοριστικά βίντεο στο youtube ή αρθρογραφεί σε blogs, είναι κάτι που θα το κρίνει και ερμηνεύσει η κοινωνιολογία και η επιστήμη της ψυχολογίας του αύριο.

Τα κοινωνικά δίκτυα έχουν αλλάξει ριζικά την κατάσταση. Σήμερα στα κοινωνικά δίκτυα, θέλουμε να επικοινωνούμε όχι μόνο με τους ξένους ή τους εικονικούς χαρακτήρες, και με ανθρώπους που γνωρίζουμε ή θέλουν να μας γνωρίσουν. Αυτό σημαίνει ότι η εικόνα μας στο δίκτυο αν μη τι άλλο, είναι ειλικρινής. Μοιραζόμαστε με φίλους, γνωστούς, συχνά και με όλο τον κόσμο, αρκετά ακριβείς πληροφορίες σχετικά με την ηλικία, τα ενδιαφέροντα μας, την τοποθεσία, τις τρέχουσες ανησυχίες, σχεδόν τα πάντα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.4 Διαρροή και ενοποίηση των πληροφοριών

Ένα πρόσφατο παράδειγμα, σχετικά με το Blippy (blippy.com), να ανταλλάσσουν πληροφορίες σχετικά με αγορές. Μια ορισμένη μέρα ο Mark ενημερώνει τον κόσμο ότι έχει αποκτήσει Θήκη για iPad με $ 41, ξόδεψε $ 24 στον Applebee εστιατόριο και $ 6450 σε μια πλαστική χειρουργική κλινική στη Φλόριντα για τη χειρουργική επέμβαση της μύτης. Μια μοναδική περίπτωση; Δεν φαίνεται. Οι Ιστοσελίδες και πίσω τους το κοινωνικό δίκτυο για την ανταλλαγή ενός ευρέος φάσματος των καθημερινών πληροφοριών αυξάνονται και απολαμβάνουν μεγάλη δημοτικότητα. Για παράδειγμα, ένα κινητό συνδεδεμένο με κοινωνικό δίκτυο που σας επιτρέπει να ανακοινώνει την τοποθεσία σας. Ή η σελίδα SpurtUp, όπου ο κόσμος μπορεί να δει πόσα push-ups έχετε κάνει σήμερα.

Αρχικά, η δημοσίευση στο Διαδίκτυο, ακόμη και αν είναι προσωπική, μοιάζει απολύτως αβλαβείς, όπως τα χόμπι, οι φωτογραφίες ή ο αριθμός των σχολείων που έχει φοιτήσει κάποιος , δεν θέτουν σε κίνδυνο. Ωστόσο, η ιστοσελίδα PleaseRobMe.com απέδειξε πώς αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για σκοπούς που δεν είναι και τόσο αβλαβείς. Αυτή η ιστοσελίδα χρησιμοποιεί τις διαθέσιμες πληροφορίες για τα δίκτυα Twitter και Τετραγωνισμού για τον εντοπισμό των κενών διαμερισμάτων, οι ιδιοκτήτες που ξοδεύουν το χρόνο μακριά από το σπίτι.

Μια άλλη πτυχή είναι ότι το εύρος της διανομής των προσωπικών σας πληροφοριών μπορεί να είναι πολύ περισσότερο από ότι αρχικά φαίνεται , ενώ συχνά δεν περιορίζονται σε ένα στενό κύκλο φίλων και γνωστών, και, επιπλέον, σχεδόν πάντα έξω από το πεδίο εφαρμογής του κοινωνικού δικτύου σας. Αυτό, με τη σειρά του, μπορεί να περιορίσει σημαντικά την ικανότητά να διατηρήσει κανείς την ανωνυμία του, όταν το θέλει.

Ξεκινώντας με το ερώτημα κατά πόσο υπάρχει η εμπιστοσύνη στη χρήση του διαδίκτυου γενικότερα μπορεί να ειπωθεί ότι η χρήση γίνεται με πλήρη ανωνυμία Φυσικά, η ιστοσελίδα που επισκέφτηκε ο χρήστης, γνωρίζει την IP διεύθυνση του υπολογιστή σας, αλλά και τι έγινε; μια ξεχωριστή τοποθεσία και απρόσωπη διεύθυνση. Φαίνεται να μην υπάρχει λόγος ανησυχίας.

Ωστόσο, πολλές, αν όχι οι πιο δημοφιλείς ιστοσελίδες χρησιμοποιούν αυτές ή άλλες τεχνολογίες για να παρακολουθούν τους επισκέπτες. Ακόμα κι αν δεν είναι μια πύλη με ένα όνομα χρήστη και τον κωδικό πρόσβασης κάθε φορά που επισκέπτεστε (και σήμερα είναι σχεδόν συνώνυμη με το Διαδίκτυο) είναι ο "εγκέφαλος" στις

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

προσωπικές πληροφορίες για τους επισκέπτες της τοποθεσίας. Για παράδειγμα, οι δημοφιλέστερες τεχνολογίες ενσωματωμένες σε "σφάλματα", με τη μορφή των εικόνων σε pixel, τα cookies ή την JavaScript εφαρμογή.

Διαρροή των ιδιωτικών πληροφοριών μπορεί να γίνει όχι μόνο στην ιστοσελίδα που επισκεφθήκατε, αλλά και σε ιστοσελίδες των τρίτων. Αυτές οι περιοχές είναι συχνά με τη μορφή κομματιών διαφήμισης. Ένα τυπικό σενάριο είναι η τοποθέτηση των διαφημίσεων όπως το Adsense της Google (googlesyndication.com, doubleclick.net), η AOL (advertising.com, tacoda.net), το Yahoo! (yieldmanager.net), σε συμφωνία με τον ιδιοκτήτη του site. Συνήθως, αυτά τα κομμάτια είναι σε μορφή στοιχείων ή απλά JavaScript γραφικές εικόνες. Η μορφή μιας σύγχρονης ιστοσελίδας περιλαμβάνει πληροφορίες με δεκάδες αιτήσεις με ερωτηματολόγια που συλλέγουν διάφορα στοιχεία, συμπεριλαμβανομένων των δικτυακών τόπων τρίτων. Αξίζει να σημειωθεί ότι αυτό συμβαίνει ανεξάρτητα από το αν ο χρήστης κάνει κλικ στο banner ή όχι.

Μια άλλη επιλογή από τρίτους παράγοντες στο χώρο είναι οι εταιρείες που προσφέρουν αναλυτικές υπηρεσίες (μεταφορές, την κυκλοφορία, τους πελάτες, τις τάσεις), όπως το google-analytics.com (Google), 2o7.net (Omniture), atdmt.com (Microsoft / aquantive), quantserve.com (Quantcast).Τέλος, το δίκτυο διανομής περιεχομένου (CDN), akamai.net, yimg.com, κλπ., τοποθετούνται εικόνες και βίντεο. Όλα αυτά τα ρεύματα, όπου οι πληροφορίες σχετικά με την επίσκεψη κάποιου εκτείνεται πολύ πιο μακριά από την τοποθεσία που επισκέφθηκε.

Κατά τη σύνοδο ολομέλειας IETF78 ο ερευνητής Balachander Krishnamurthy της AT & T Labs-Research έδωσε μια ενδιαφέρουσα παρουσίαση για το θέμα της διαρροής των προσωπικών πληροφοριών στο διαδίκτυο.[xix] Η παρουσίαση αυτή βασίζεται στα χρόνια της έρευνας που διεξάγεται μαζί με τον Craig E. Διαθήκες του Worcester Polytechnic Institute. Οι επιστήμονες έχουν μελετήσει το λεγόμενο "σημείο εμπιστευτικότητας", που καθορίζει το βαθμό διάδοσης των πληροφοριών στους χρήστες σε ξένους τόπους. Η μελέτη αποτελείται από εννέα πειράματα, που καλύπτουν μια περίοδο 5 ετών, τα 1200 πιο δημοφιλή sites σε διάφορες κατηγορίες, 68 χώρες και 19 γλώσσες[2].

Μία από τις παραμέτρους που διερευνώνται είναι οι λεγόμενες ενώσεις του τόπου που επισκέπτεται κάποιος μέσω ιστοσελίδων τρίτων. Για παράδειγμα, αν δύο ανεξάρτητες ιστοσελίδες χρησιμοποιούν το Google-analytics.com, σχετίζονται. Τα

[2] σύμφωνα με την άποψη της Alexa, στο http://www.alexa.com/

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αποτελέσματα ήταν αρκετά περίεργα. Το 70% του συνόλου των ερωτηθέντων επισκέπτεται μια ένωση με περισσότερους από 400 ξένους τόπους.

Αλλά το πιο εντυπωσιακό ήταν ο βαθμός συγκέντρωσης των τόπων τρίτων μερών. Μόνο 10 από τους μεγαλύτερους δικτυακούς τόπους τρίτων (doubleclick.net, google-analytics.com, 2mdn.net, quantserve.com, scorecardresearch.com, atdmt.com, omniture.com, googlesyndication.com, yieldmanager.com, 2o7.net) ήταν εκπροσωπούμενη από 78,5% του συνόλου των τοποθεσιών.

Αλλά δεν είναι μόνο αυτό. Ανάλυση των αγορών και των συγχωνεύσεων των επιχειρήσεων του τομέα αυτού της αγοράς επέτρεψε στους ερευνητές να συνδυάζουν περισσότερες από αυτές τις τοποθεσίες στις τρεις μεγάλες οικογένειες: - Google, η οποία περιλαμβάνει, για παράδειγμα, doubleclick.net, googlesyndication.com και google-anaystics.com - Adobe, όπου οι μεγαλύτεροι εκπρόσωποι είναι Omniture. com, και offermatica.com hitbox.com, και - Miscrosoft, με μεγαλύτερη εξαγορά της - Aquantive - το 2007.Λιγότερο σημαντική, αλλά και αξιοσημείωτη είναι η "οικογένεια" Yahoo και AOL.Παρακολουθείται η εξάπλωση αυτών των οικογενειών να επισκέπτονται τοποθεσίες έχει δείξει τη συνεχή ανάπτυξη και αύξηση της, με 40% το 2005 σε 84% τον Μάρτιο του 2010.

Το βάθος της διείσδυσης έχει επίσης αυξηθεί. Αυτό σημαίνει ότι ο χρήστης παρακολουθείτε στις επισκέψεις σε περισσότερες από μία οικογένεια από ιστοσελίδες τρίτων. Έτσι, στη διάθεση των εταιρειών που παρέχουν τις υπηρεσίες αυτές, υπάρχει μια τεράστια ποσότητα πληροφοριών σχετικά με τους χρήστες στο Διαδίκτυο, καθώς και η δυνατότητα να συσχετιστούν τα δεδομένα σχετικά με τις επισκέψεις σε ανεξάρτητους χώρους για να δημιουργηθεί ένα "προφίλ" του χρήστη να καθορίσει τις προτιμήσεις του, τις συνήθειες, συμπεριφορές, τοποθεσίες και άλλα προσωπικά δεδομένα.

Ωστόσο, όταν λέμε "χρήστης", στις περισσότερες περιπτώσεις είναι ένα δαχτυλίδι-διεύθυνση IP του υπολογιστή ή των υπολογιστών στους οποίους ο χρήστης εργάζεται. Με άλλα λόγια, μπορείτε να πάρετε αρκετά αξιόπιστες πληροφορίες για ένα συγκεκριμένο χρήστη, αλλά χωρίς να γνωρίζεται το όνομα του.

4.5 Διαρροή εμπιστευτικών πληροφοριών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Αυτό είναι το επιχείρημα που χρησιμοποιείται συχνά από τις εταιρείες που παρέχουν υπηρεσίες σε τρίτους. Ωστόσο, ο Balachander Krishnamurthy και Craig E. μελέτησαν το θέμα με περισσότερες λεπτομέρειες και δείχνουν ότι ο «χρήστης» μπορεί να εντοπιστεί μέσω των κοινωνικών δικτύων [xx]. Είναι γνωστό πλέον ότι οι περισσότεροι ιστότοποι κοινωνικής δικτύωσης χρησιμοποιούν τις υπηρεσίες τρίτων, που μόλις περιγράφτηκε. Αυτή η τοποθέτηση των διαφημίσεων, το περιεχόμενο, και μια ποικιλία των φυλλομετρητών και ιχνηλάτες τα οποία παρακολουθούν την κίνηση του χρήστη στο δικτυακό χώρο.

Φυσικά, η ποσότητα των πληροφοριών που μπορούν να ληφθούν για τον χρήστη, γνωρίζοντας την ταυτότητα του, εξαρτάται από τις ρυθμίσεις του δικτύου και των χρηστών, αλλά η ανάλυση από τα πιο δημοφιλή δίκτυα από τους ίδιους ερευνητές έδειξε ότι το όνομα, προσωπική φωτογραφία, το φύλο, τα χόμπι, η λίστα των φίλων, της εκπαίδευσης γίνονται γνωστά ευκολότερα στις περισσότερες υποθέσεις.

Τώρα ο τρίτος μπορεί να συνδέσει διάφορα χαρακτηριστικά των χρηστών, όπως η διεύθυνση IP του υπολογιστή, με τον ειδικό χαρακτήρα των κοινωνικών δικτύων. Η ένωση αυτή μπορεί να καθοριστεί με το cookie-tracker, όπως συχνά διαβιβάζονται στην αίτηση. Δεδομένου ότι οι cookie-tracker έχουν συνήθως μεγάλη διάρκεια ζωής (π.χ., η ισχύς των cookies μπορεί να είναι ακόμη και ένα έτος), το παρελθόν ,το μέλλον και η τωρινή διαδρομή του χρήστη μπορεί να σχετίζονται με αυτό το χαρακτήρα, και έτσι εντοπίζεται.

Λαμβάνοντας υπόψη το βαθμό του συνεταιρίζεσθαι χώρων και τη συγκέντρωση των ιστοσελίδων τρίτων, η δυνατότητα σε τρίτους να παρακολουθούν τα «προφίλ» των χρηστών του Διαδικτύου είναι σημαντική. Σίγουρα δεν είναι το γεγονός ότι τα τρίτα μέρη παράγουν ή χρησιμοποιούν μια παρόμοια ένωση, αλλά η πιθανότητα αυτή υπάρχει. Δεδομένου ότι οι περισσότερες ιστοσελίδες τρίτων που ανήκουν σε επιχειρήσεις σε ένα ή τον άλλο τρόπο συνδέονται με τον κλάδο της διαφήμισης, οι δυνατότητες αυτές είναι απίθανο να χρησιμοποιηθεί για πολιτικούς ή εγκληματικούς σκοπούς. Το φαινόμενο "Big Brother" είναι μέρος της σημερινής, εμπορευματοποιημένης πραγματικότητας προσφέροντάς μας όλο και πιο πολύπλοκες διαφημίσεις, όπως πάντα, οι οποίες προσπαθούν όλο και περισσότερο να επηρεάσουν τις επιλογές μας .

Περιττό να πούμε, ότι οι χρήστες των μηχανών αναζήτησης στην Κίνα και άλλα ολοκληρωτικά καθεστώτα πρέπει να σκέφτονται αρκετά πριν ψάξουν για πληροφορίες σχετικά με δημοφιλής ομάδες της αντιπολίτευσης ή ιστορικά

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

γεγονότα.[3]Ενας χρήστης εισέρχεται με ένα ερώτημα αναζήτησης, όπως "δωρεάν Ταϊβάν» στην Κίνα ή "Ισλαμική Τζιχάντ" στην Αίγυπτο μπορεί να τιμωρηθεί για την περιέργεια του . Ωστόσο, αυτή η λογοκρισία θα πλήττει όχι μόνο της κοινωνίες όπου η δημοκρατία και η ελευθερία του λόγου είναι λιγοστές, αλλά και δυτικές δημοκρατίες.[xxi]

4.6 Μέθοδος : ανάλυση κίνησης

Ένας τρόπος που μπορούν να χρησιμοποιηθούν οι πληροφορίες αυτές που μαζεύει μια μηχανή αναζήτησης λέγεται *ανάλυση κίνησης*. Καθώς γενικώς δεν αποτελεί μια απειλή για την ιδιωτικότητα συγκεκριμένων ατόμων, είναι αδιαμφισβήτητα ένα πολύ σοβαρό θέμα σχετικά με το πώς χρησιμοποιούνται οι πληροφορίες που κρατάει μια μηχανή αναζήτησης. Η ανάλυση κίνησης λειτουργεί ως εξής – χρησιμοποιώντας τις πληροφορίες σχετικά με αναζητήσεις όπως την τοποθεσία του χρήστη, και το θέμα της αναζήτησης, μπορεί να δημιουργήσει μια μηχανή αναζήτησης μια εικόνα, για παράδειγμα, που δείχνει ότι ένα συγκεκριμένο προϊόν χρησιμοποιείται πιο συχνά σ'έναν τόπο. Προφανώς, το να μπορεί, μια μηχανή αναζήτησης, να κάνει πράξη αυτές τις εφαρμογές, μπορεί εύκολα να γίνει επικίνδυνο – ο έλεγχος που έχει η μηχανή αναζήτηση σημαίνει ότι θα μπορούσε να επιδρά σε εκλογές, τιμές μετοχών, και άλλα σημαντικά θέματα.

Αυτή η μέθοδος (ανάλυση κίνησης) χρησιμοποιεί ένα είδος πληροφοριών που λέγεται Προσωπικά Προσδιοριστικές Πληροφορίες, ή ΠΠΠ. Τέτοιες πληροφορίες περιέχουν, σχετικά με ηλεκτρονικές αναζητήσεις, την πηγή της αναζήτησης, τον προορισμό, και το θέμα της αναζήτησης. Σύμφωνα με την Κοινοπραξία του Παγκοσμίου Ιστού, πολιτικές ιδιωτικότητας δέχονται άθροιση δεδομένων, με στατιστικά πάνω στις αναζητήσεις αλλά όχι συγκεκριμένα δεδομένα. Αυτό όμως δεν αποκλείει τη χρήση των πληροφοριών για σκοπούς όπως τους προαναφερθέντες.

[3] Lester Haines, Αιγύπτιος ιδιωκτήτης προσωπικής ισοτσελίδας ο οποίος φυλακίστηκε για τέσσερα χρόνια, THE REGISTER, Feb. 22, 2007, το άθρο είναι διαθέσιμο στον σύνδεσμο: http://www.theregister.co.uk/2007/02/22/egyptian_blogger_jailed. Thompson, supra note 96.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.7 Θέματα ασφάλειας που προκύπτουν για τους χρήστες (και παραδείγματα που έχουν ήδη προκύψει)

Η μηχανή αναζήτησης Google δίνεται ως παράδειγμα σαν μια μηχανή αναζήτησης η οποία διατηρεί τα στοιχεία που καταχωρούνται για την περίοδο των τριών τετάρτων του έτους, πριν καταστεί άνευ αντικειμένου για δημόσια χρήση. Το Yahoo! ακολουθεί τα βήματα της Google με την έννοια ότι διαγράφει επίσης πληροφορίες για το χρήστη μετά από μια περίοδο ενενήντα ημερών. Άλλες μηχανές αναζήτησης όπως ASK! μηχανή αναζήτησης έχει προωθήσει ένα εργαλείο "AskEraser", το οποίο επαναλαμβάνει κατ 'ουσίαν μακριά προσωπικές πληροφορίες όταν τους ζητηθεί. [xxii]

Κάθε αρχεία καταγραφής αναζήτησης των χρηστών αποτελούν "προσωπικά δεδομένα"; Μπορεί τα δεδομένα στα αρχεία καταγραφής αναζήτησης να ανιχνευθούν σε συγκεκριμένα άτομα;

Αυτό μπορούμε να δούμε ότι το κάνουνε, και επομένως εν μέρει παραβιάζουν την ιδωτικότητα. Πρώτον, όπως προαναφέρθηκε, οι μηχανές αναζήτησης διατηρούν την Διεύθυνση IP την οποία έχει ο χρήστης όταν θέτει τα ερωτήματά του στην μηχανή αναζήτησης. Η διεύθυνση IP είναι μια μοναδική σειρά από αριθμούς που έχουν αντιστοιχιστεί στον υπολογιστή ενός χρήστη από τον Πάροχο Υπηρεσιών Διαδικτύου της (ISP) για να επικοινωνούν με τον υπολογιστή της για το δίκτυο.[xxiii]

Στην πραγματικότητα, το ισοδύναμο για τον κυβερνοχώρο μίας IP είναι στον πραγματικό κόσμο ο δρόμος, η διεύθυνση ή ο αριθμός τηλεφώνου. Μια διεύθυνση IP μπορεί να είναι δυναμική, δηλαδή μια διαφορετική διεύθυνση εκχωρείται σε ένα χρήστη κάθε φορά που θα συνδεθεί με το δίκτυο ή στατικό, δηλαδή ανατεθεί σε έναν υπολογιστή με έναν ISP να είναι μόνιμη διεύθυνση στο Διαδίκτυο. Το ερώτημα αν μια διεύθυνση IP αποτελεί «προσωπικά δεδομένα» έχει συζητηθεί πολύ στα πλαίσια της ΕΕ.[xxiv] Η απάντηση εξαρτάται από το αν η διεύθυνση μπορεί να συνδέεται με ένα "προσδιορισμένο ή προσδιορισμό φυσικού προσώπου", μέσω εύλογου μέσου.[xxv]

Σαφώς, μια στατική διεύθυνση είναι πιο "προσωπική" από μια δυναμική διεύθυνση και σε κάθε περίπτωση, μια διεύθυνση είναι πιο "προσωπική" στην κατοχή ενός ISP,ο οποίος έχει την ικανότητα να συνδεθεί με τα στοιχεία εγγραφής ενός συγκεκριμένου χρήστη, και να βρει όλες τις πληροφορίες του κατόχου της.[xxvi]

Το ευρωπαϊκό παρατηρητήριο της προστασίας των δεδομένων, στο άρθρο 29

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ομάδα Εργασίας, πρόσφατα αποφάνθηκε ότι αποτελούν ακόμη και οι δυναμικές διευθύνσεις IP "Προσωπικά δεδομένα". Δήλωσε ότι «αν ο ISP είναι σε θέση να διακρίνει με απόλυτη βεβαιότητα ότι τα δεδομένα αντιστοιχούν σε χρήστες που μπορούν να προσδιοριστούν, θα πρέπει να μεταχειρίζεται όλες τις πληροφορίες IP ως δεδομένα προσωπικού χαρακτήρα, ώστε να είναι στην ασφαλείς οι χρήστες . "[xxvii]

Κατά συνέπεια, ακόμη και αν η Google δεν θα μπορούσε να συνδέει μια διεύθυνση IP (και επομένως να σύνδεση και την αναζήτηση) προς ένα συγκεκριμένο πρόσωπο, το γεγονός ότι οι πάροχοι έχουν τέτοια δυνατότητα και ότι η κυβέρνηση μπορεί να τα αναζητήσει τα καθιστά καταγραφή "προσωπικών δεδομένων" και η παραβίαση αντιτίθεται στην έννοια της ιδιωτικότητας.

Ένας κορυφαίος υπερασπιστής των ανθρωπίνων δικαιωμάτων, η Privacy International, κατηγόρησε πρόσφατα την Google για πρακτικές παραβίασης της ιδιωτικότητας ως τη χειρότερη από περισσότερους από 20 κορυφαίους παροχούς υπηρεσιών Διαδικτύου, συμπεριλαμβανομένων των Microsoft, Yahoo, Amazon και eBay.[xxviii]

Η Privacy International περιγράφει την Google ως «ενδημική απειλή για την προστασία της ιδιωτικής ζωής."[xxix] Επικρίνει την «επιθετική χρήση της σε βάθος ή δυνητικά χωροκατακτητικών τεχνολογίες και τεχνικές» της Google και υποστηρίζει ότι η εταιρεία «δεν ακολουθεί τη γενικά αποδεκτή πρακτική της ιδιωτικότητας, όπως έχουν ορίσει οι κατευθυντήριες γραμμές του ΟΟΣΑ και της Προστασίας Προσωπικών Δεδομένων στοιχεία της κοινοτικής νομοθεσίας για την προστασία των δεδομένων."[xxx] Οι Ρυθμιστικές αρχές της ΕΕ περί προστασίας των δεδομένων έχουν ξεκινήσει πρόσφατα μια έρευνα σχετικά με τη διατήρηση των δεδομένων της Google και τις πρακτικές προστασίας της ιδιωτικής ζωής,[4] η οποία πολύ γρήγορα επεκτάθηκε για να καλύψει άλλες μηχανές αναζήτησης.[xxxi]

Και το Ηλεκτρονικό Κέντρο Πληροφόρησης Προστασίας Προσωπικών Δεδομένων (EPIC), μια κορυφαία ομάδα της ιδιωτικότητας, κατέθεσε καταγγελία στην Ομοσπονδιακή Επιτροπή Εμπορίου, υποστηρίζοντας ότι το ενδεχόμενο της

[4] Πρόταση που είχε αποστήλει η ομάδα εργασίας του άθρου 29 στον Peter Fleischer, υπεύθυνο σύμβουλο για θέματα ιδιωτικότητας της google. Και το οποίο είναι διαθέσιμο στην διεύθυνση:http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_16_05_07_en.pdf;

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συγχώνευσης της Google Doubleclick πρέπει να αποκλειστεί.[xxxii] Η Google με την πρόσφατη εξαγορά της DoubleClick .Η DoubleClick είναι κορυφαία εταιρεία στον τομέα της online διαφήμισης. Τα αποτελέσματα βασίζονται στην παρακολούθηση της συμπεριφοράς των χρηστών σε όλη τον κυβερνοχώρο και την τοποθέτηση διαφημιστικών banners σε ιστοσελίδες. Η εταιρεία είναι εδώ και πολύ καιρό αντιτίθεται στους υποστηρικτές της ιδιωτικότητας και της προστασίας προσωπικών δεδομένων.[xxxiii]

Τον Φεβρουάριο του 2000, η EPIC, κατέθεσε καταγγελία στην FTC ισχυριζόμενη ότι η DoubleClick παρακολουθούσε παράνομα τις online δραστηριότητες των χρηστών. Επειδή δημιουργούσε μια αντιστοίχιση των προσωπικών περιηγήσεων στον παγκόσμιο ιστό με πληροφορίες από προσωπικά προφίλ. Όλα αυτά τα στοιχεία τα διατηρούσε σε μια εθνική βάση δεδομένων για τις ανάγκες του μάρκετινγκ.[5]

Η υπόθεση κατέληξε σε μια διευθέτηση, σύμφωνα με την οποία η DoubleClick ανέλαβε μια σειρά από δεσμεύσεις για τη βελτίωση των πρακτικών της συλλογής δεδομένων, για την αύξηση της διαφάνειας και παροχή στους χρήστες επιλογές εξαίρεσης από την υπηρεσία καταγραφής δεδομένων.[xxxiv]

Η Double Click συνεχίζει να χρησιμοποιεί cookies τρίτων[6] καθώς και την τεχνολογία "DART" του (Dynamic, Διαφήμιση, Αναφορά και στόχευσης) τεχνολογία για να παρακολουθεί τη δραστηριότητα του χρήστη σε πολλαπλούς δικτυακούς τόπους.

Στην πρόσφατη καταγγελία της προς την Ομοσπονδιακή Επιτροπή Εμπορίου σχετικά με το Google-Double Click συγχώνευση, η EPIC ισχυρίστηκε ότι με την αγορά

[5] Στο θέμα της DoubleClick, Καταγγελία και Αίτηση ασφαλιστικών μέτρων, Αίτηση για την Έρευνα από την Ομοσπονδιακή Επιτροπή Εμπορίου (07/08/2012), διαθέσιμο στο http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[6] Ενώ τα cookies μόνο αποστέλλονται στο διακομιστή δημιουργίας τους ή ένα στον ίδιο τομέα Internet, web σελίδα μπορεί να περιέχει εικόνες ή άλλα στοιχεία είναι αποθηκευμένα σε διακομιστές και σε άλλους τομείς. Τα cookies που έχουν οριστεί κατά τη διάρκεια της ανάκτησης αυτών των συστατικών ονομάζονται cookies τρίτων. Διαφημιστικές εταιρείες χρησιμοποιούν άλλους κατασκευαστές cookies για να παρακολουθούν ένα χρήστη σε πολλές τοποθεσίες πληροφορίες από αναζήτηση στο http://en.wikipedia.org/wiki/HTTP_cookie.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Double click, η Google επεκτείνει την ικανότητά της να παρακολουθεί τους χρήστες όχι μόνο στην ιστοσελίδα της, αλλά και στον κυβερνοχώρο.[7]

Το σύστημα της AOL είναι ένα άλλο παράδειγμα. Η AOL έχει μια βάση δεδομένων με 21 εκατομμύρια μόνιμα μέλη, το καθένα με τον δικό του αριθμό. Η Ο τρόπος που η μηχανή αναζήτησης της AOLSearch έχει συσταθεί, δίνει τη δυνατότητα στην AOL να διατηρεί αρχεία όλων των ιστιοχώρων που επισκέπτεται οποιοδήποτε μέλος της. Ακόμη και αν η πραγματική ταυτότητα του χρήστη δεν είναι γνωστή, δημιουργείται ένα πλήρες προφίλ μέλους με την συλλογή και την αποθήκευση από τις πληροφορίες αναζητήσεις του χρήστη .Με την χρήση των αρχείων που οι χρήστες έχουν δημιουργηθεί με τα ερωτήματά τους μέσω του AOLSearch, μπορούμε να μάθουμε αμέτρητες πληροφορίες για κάποιον που δεν γνωρίζουμε καν το όνομά του. [xxxv]

Προκειμένου να αντιμετωπίσουν το τι θεωρείται μια σοβαρή απειλή στην ιδωτικότητα, οι διάφοροι νομικοί θεσμοί έχουν παράγει κάποιους νόμους ώστε να προστατεύονται τα δικαιώματα και η ιδωτικότητα των χρηστών του διαδικτύου.

Επιπρόσθετα, οι μηχανές αναζήτησης έχουν φτιάξει και τις δικές τους πολιτικές σχετικά με την προστασία των προσωπικών δεδομένων. Αυτές οι πολιτικές έχουν δημιουργηθεί ως αποτέλεσμα της επιθυμίας των χρηστών λόγω της έλλειψης νομικής προστασίας, και εφαρμόζονται μέσω των όρων χρήσης που έχει η κάθε μηχανή αναζήτησης – δηλαδή, όταν χρησιμοποιεί κάποιος μια μηχανή αναζήτησης, δείχνει ότι συμφωνεί με το πώς η μηχανή αναζήτησης θα χρησιμοποιεί οποιαδήποτε πληροφορία.

4.8 Υπάρχουσες προβληματικές καταστάσεις (παράδειγμα google με την συνένωση του google search)

[7] Καταγγελία και Αίτηση ασφαλιστικών μέτρων Επίσης δείτε Στο θέμα της Google και DoubleClick, Συμπληρωματικά Υλικά για την ενίσχυση της Εν αναμονή Καταγγελία και Αίτηση ασφαλιστικών μέτρων, ζητώντας να διεξαχθεί έρευνα και για άλλες Αρωγής, (6 Ιούνη, 2007), διαθέσιμο στο http://www.epic.org/privacy/ftc/google/supp_060607.pdf; Canadian Internet Policy and Public Interest και http://www.cippic.ca/uploads/Google-DC_s.9_CompAct_complaint_FINAL.pdf.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Στις αλλαγές που έγιναν στις μηχανές αναζήτησης στο διαδίκτυο περιλαμβάνεται εκείνη της μηχανής αναζήτησης της Google. Ξεκινώντας το 2009, η Google άρχισε να τρέχει ένα νέο σύστημα όπου η αναζήτηση έγινε εξατομικευμένη. Το στοιχείο που ερευνάται και τα αποτελέσματα που εμφανίζονται θυμάται τις προηγούμενες πληροφορίες που σχετίζονται με το άτομο. Η μηχανή αναζήτησης της Google δεν είναι μόνο ότι επιδιώκει την αναζήτηση, αλλά προσπαθεί επίσης να επιτρέψει στο χρήστη να αισθανθεί όπως η μηχανή αναζήτησης αναγνωρίζει τα συμφέροντά του. Αυτό επιτυγχάνεται με τη χρήση της online διαφήμισης.[xxxvi]

Ένα σύστημα που χρησιμοποιεί η Google για να φιλτράρει τις διαφημίσεις και τα αποτελέσματα αναζήτησης που θα μπορούσαν να ενδιαφέρουν το χρήστη είναι από την κατοχή ενός συστήματος κατάταξης, που ελέγχει τη σχετικότητα που περιλαμβάνει την παρατήρηση της συμπεριφοράς των χρηστών, ενώ κάνουν αναζήτηση. Μια άλλη λειτουργία των μηχανών αναζήτησης είναι η προβλεψιμότητα της θέσης. Οι μηχανές αναζήτησης είναι σε θέση να προβλέψουνε ποια είναι η τοποθεσία του χρήστη από τον εντοπισμό διευθύνσεων IP και τις γεωγραφικές περιοχές.[xxxvii]

Η Google είχε δηλώσει δημοσίως στις 24 Ιανουαρίου του 2012, ότι η πολιτική προστασίας της ιδιωτικής ζωής της θα αλλάξει και πάλι . Αυτή η νέα πολιτική θα αλλάξει τα ακόλουθα για τους χρήστες της: (1) η πολιτική προστασίας προσωπικών δεδομένων θα γίνει πιο σύντομη και πιο εύκολη να κατανοηθεί και (2) η πληροφορία που παρέχετε στους χρήστες θα χρησιμοποιείται με περισσότερους τρόπους από ότι χρησιμοποιείται σήμερα. Ο στόχος της Google είναι να καταστήσει την εμπειρία των χρηστών καλύτερη από ότι είναι σήμερα.[xxxviii]

Αυτή η νέα πολιτική προστασίας της ιδιωτικής ζωής έχει προγραμματιστεί να τεθεί σε ισχύ από την 1η Μαρτίου του 2012. Ο Peter Fleischer, σύμβουλος του Παγκόσμιου απορρήτου για την Google, εξήγησε ότι αν ένα άτομο έχει συνδεθεί στο λογαριασμό του, και μόνο αν αυτός έχει συνδεθεί, οι πληροφορίες θα συγκεντρώνονται από διάφορες υπηρεσίες της Google με τον οποίο αυτός έχει χρησιμοποιηθεί προκειμένου να είναι πιο ελαστικοί. Η νέα πολιτική απορρήτου της Google θα συνδυάζει όλα τα δεδομένα που χρησιμοποιούνται στις μηχανές αναζήτησης της Google (π.χ., το YouTube και το Gmail), προκειμένου να εργαστούν προς την κατεύθυνση των συμφερόντων ενός ατόμου. Ένα πρόσωπο που, στην

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πραγματικότητα, θα είναι σε θέση να βρείτε ότι αυτός θέλει με πιο αποτελεσματικό τρόπο, επειδή ποσοστό όλοι έψαχναν της πληροφόρησης σε περιόδους σύνδεσης θα βοηθήσει να περιορίσετε τα νέα αποτελέσματα αναζήτησης.[xxxix]

4.9 Η πολιτική απορρήτου της Google και άλλων εταιρειών

Η πολιτική απορρήτου της Google εξηγεί για τις πληροφορίες που συλλέγουν και γιατί τις συλλέγουν, πώς τις χρησιμοποιούν, και πώς έχουν πρόσβαση και ενημέρωση των πληροφοριών. Η Google θα συλλέγει πληροφορίες για την καλύτερη εξυπηρέτηση των χρηστών της, όπως η γλώσσα τους, ποιες διαφημίσεις θα είναι χρήσιμες για τους ανθρώπους που είναι συνδεδεμένοι στο λογαριασμό τους. Η Google ανακοινώνει ότι θα χρησιμοποιήσει αυτές τις πληροφορίες για την παροχή, τη διατήρηση, την προστασία της Google και των χρηστών της. Οι πληροφορίες που χρησιμοποιεί η Google θα παρέχουν στους χρήστες πιο σχετικά αποτελέσματα αναζήτησης και διαφημίσεις. Η νέα πολιτική προστασίας προσωπικών δεδομένων εξηγεί ότι η Google μπορεί να χρησιμοποιήσει και να ανταλλάζει πληροφορίες σχετικά με μία υπηρεσία με άλλες υπηρεσίες της Google, θα αντιμετωπίζει το χρήστη ως ένα μεμονωμένο χρήστη σε όλα τα προϊόντα της. Η Google υποστηρίζει ότι η νέα πολιτική προστασίας προσωπικών δεδομένων θα ωφελήσει τους χρήστες της διότι θα είναι πιο εύκολη στην χρήση της.

Η Google θα είναι σε θέση να διορθώσει την ορθογραφία του ονόματος του φίλου ενός χρήστη σε μια αναζήτηση ή να ειδοποιεί το χρήστη ότι είναι αργά βασιζόμενη στο ημερολόγιό τους και την τρέχουσα θέση.

Ακόμα κι αν η Google ενημερώνει την κατάσταση της ιδιωτικής τους ζωής, οι κατευθυντήριες γραμμές για την προστασία της ιδιωτικότητας δεν θα αλλάξουν. Για παράδειγμα, η Google δεν πωλεί τις προσωπικές πληροφορίες και ούτε τις διαμοιράζει σε εξωτερικούς παράγοντες.[xl]

Η νέα πολιτική απορρήτου της Google προκαλεί πολλές ανησυχίες και ζητήματα στους χρήστες και τους δημόσιους υπαλλήλους. Η κύρια ανησυχία αφορά την ανταλλαγή δεδομένων από πολλαπλές πηγές. Επειδή αυτή η πολιτική συγκεντρώνει όλες τις πληροφορίες και τα στοιχεία αναζητούνται από πολλαπλές μηχανές όταν

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κάποιος είναι συνδεδεμένος και χρησιμοποιούνται για να βοηθήσει τους χρήστες. Οι δημόσιοι υπάλληλοι και οι χρήστες του Google λογαριασμού ανησυχούν για τη διαδικτυακή ασφάλεια, λόγω όλων αυτών των στοιχείων που συγκεντρώνονται από διάφορες πηγές.[xli]

Ορισμένοι χρήστες δεν αντιμετωπίζουν θετικά την πολιτική προστασίας προσωπικών δεδομένων, και επιθυμούν να διατηρήσουν την υπηρεσία της Google ξεχωριστά. Η ενημέρωση για την πολιτική απορρήτου της Google έχει ανησυχήσει τόσο το δημόσιο όσο και τον ιδιωτικό τομέα. Η Ευρωπαϊκή Ένωση έχει ζητήσει από την Google να καθυστερήσει την έναρξη της νέας πολιτικής προστασίας της ιδιωτικότητας, προκειμένου να διασφαλίσει ότι δεν παραβιάζει το κοινοτικό δίκαιο. Η κίνηση αυτή είναι σύμφωνη με άλλα ξένα κράτη, όπου η επιτήρηση είναι πιο διεξοδική και σε μεγάλύτερο βαθμό, τα οποία έχουν αρκετές αντιρρήσεις ως προς τη μείωση της ασφάλειας και της ιδιωτικότητας σε απευθείας σύνδεση.[xlii] Ο Καναδάς και η Γερμανία έχουν κάνει αρκετές έρευνες τόσο σχετικά με τη νομιμότητα της τόσο στο Facebook, κατά τις αντίστοιχες πράξεις της ιδιωτικής ζωής, το 2010. Η νέα πολιτική προστασίας της ιδιωτικής ζωής αυξάνει μόνο άλυτα προβλήματα όσον αφορά την προστασία της ιδιωτικής ζωής των χρηστών. [xliii]Ενα επιπλέον χαρακτηριστικό της ανησυχίας για τη νέα πολιτική απορρήτου της Google είναι η φύση της πολιτικής. Κάποιος πρέπει να αποδεχτεί όλα τα χαρακτηριστικά ή να διαγράψει τους υπάρχοντες λογαριασμούς της Google. [xliv]Η ενημέρωση θα επηρεάσει το Google + κοινωνικό δίκτυο, κάνοντας έτσι το Google + τις ρυθμίσεις σε αντίθεση με άλλες προσαρμόσιμους δικτυακούς τόπους κοινωνικής δικτύωσης. Η προσαρμογή των ρυθμίσεων απορρήτου του κοινωνικού δικτύου είναι η βασική τακτική που για πολλούς θεωρείται απαραίτητη για ιστότοπους κοινωνικής δικτύωσης. Αυτή η ενημερωμένη έκδοση του συστήματος έχει κάνει αρκετούς χρήστες της Google να δυσπιστούν όσον αφορά τη συνέχιση των υπηρεσιών.[xlv] Επιπλέον, ορισμένοι φοβούνται ότι η ανταλλαγή δεδομένων μεταξύ των υπηρεσιών της Google θα μπορούσε να οδηγήσει σε αποκαλύψεις των ταυτοτήτων. Πολλά ψευδώνυμα που χρησιμοποιούν οι ανησυχίες για τη δυνατότητα αυτή, και να υπερασπιστεί τον ρόλο των ψευδωνύμων στη λογοτεχνία και ιστορία. [xlvi]

Υπάρχουν ορισμένες λύσεις που είναι σε θέση να προστατεύσουν το απόρρητο του χρήστη στο διαδίκτυο και περιλαμβάνουν και προγράμματα όπως το "Rapleaf", το οποίο είναι μια ιστοσελίδα που έχει μια μηχανή αναζήτησης που επιτρέπει στους

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

χρήστες να κάνουν όλες τις αναζητήσεις διατηρώντας τις προσωπικές πληροφορίες ιδιωτικές. Άλλες ιστοσελίδες που δίνουν, επίσης, αυτή την επιλογή στους χρήστες τους είναι το Facebook και το Amazon[xlvii]. Άλλες μηχανές αναζήτησης όπως DuckDuckGo δεν αποθηκεύουν προσωπικά δεδομένα.

4.10 Οι ενέργειες της Ομάδα Εργασίας του Άρθρου 29 για την ιδιωτικότητα στις μηχανές αναζήτησης.

Η συγκεκριμένη ομάδα έχει γνωμοδοτήσει και σε συγκεκριμένα θέματα που αφορούν τις μηχανές αναζήτησης. Σε αυτό πλαίσιο λειτουργίας της, η Ομάδα Εργασίας του Άρθρου 29 της Οδηγίας 95/46/ΕΚ για την προστασία των προσωπικών δεδομένων εξέδωσε τον Απρίλιο του 2008 Γνώμη για θέματα προστασίας προσωπικών δεδομένων που σχετίζονται με μηχανές αναζήτησης, στη διαμόρφωση της οποίας συμμετείχε και η ελληνική Αρχή.

Αρχικά η ομάδα κάνει την εξής παρατήρηση: ότι η αυξανόμενη ανάγκη για αναζήτηση πληροφορίας στις ημέρες μας, έχουν κάνει τις μηχανές αναζήτησης μέρος της καθημερινότητας των χρηστών του Διαδικτύου ως βασικό εργαλείο αναζήτησης και ανάκτησης πληροφορίας. Το ζήτημα το οποίο τίθεται όμως, είναι ο μεγάλος όγκος των προσωπικών δεδομένων που διατηρούν κυρίως μέσω των αρχείων καταγραφής των αναζητήσεων (search logs), που πραγματοποιούν οι χρήστες. Οι πληροφορίες που περιέχονται στα προαναφερθέντα logs, μπορούν να οδηγήσουν ακόμα και στην αναγνώριση του χρήστη όπως π.χ. το ίδιο το ερώτημα της αναζήτησης, την IP διεύθυνση του χρήστη, την ώρα και μέρα της αναζήτησης, το λειτουργικό σύστημα του υπολογιστή του χρήστη, τη γλώσσα που χρησιμοποιήθηκε, τα cookies ή άλλα συναφή προγράμματα που έχουν εγκατασταθεί στον υπολογιστή του χρήστη, κ.α. Βάση της συχνότητας των αναζητήσεων του χρήστη και των προτιμήσεών του, οι μηχανές αναζήτησης δημιουργούν ένα προφίλ του χρήστη με σκοπό τη διαφήμιση, με αποτέλεσμα όμως να επηρεάζουν την ιδιωτική του ζωή, ειδικά στις περιπτώσεις που τα δεδομένα των αναζητήσεων είναι ελλιπή, λανθασμένα ή υπερβολικά.

Ένα βασικό συμπέρασμα που προκύπτει από την ανωτέρω Γνώμη είναι ότι η Οδηγία για την προστασία των προσωπικών δεδομένων (95/46/ΕΚ) ισχύει γενικά, ακόμα και

όταν η επεξεργασία των προσωπικών δεδομένων γίνεται από μηχανές αναζήτησης που εδρεύουν σε χώρα εκτός της Ευρωπαϊκής Ένωσης (όπως οι μεγάλες αμερικανικές μηχανές αναζήτησης Google, Yahoo!, κ.α.). Η Οδηγία όμως σχετικά με την διατήρηση των δεδομένων (2006/24/ΕΚ), δεν εφαρμόζεται στην περίπτωση των παρόχων υπηρεσιών μηχανών αναζήτησης και επιπρόσθετα οι μηχανές αναζήτησης μπορούν να επεξεργάζονται προσωπικά δεδομένα μόνο για μόνιμους σκοπούς.

Έτσι λοιπόν, αν η συλλογή των προσωπικών δεδομένων δεν εξυπηρετεί τον νόμιμο σκοπό για τον οποίο είχαν συλλεχθεί, θα πρέπει να διαγράφεται από τους παρόχους τέτοιων υπηρεσιών, μόνιμα ή να διατηρούν την ανωνυμία του χρήστη. Αυτό θα πρέπει να είναι μη αναστρέψιμο και όποτε υπάρχει διατήρηση των δεδομένων στα cookies θα πρέπει να είναι σε θέση να το αιτιολογήσουν. Η συγκατάθεση του χρήστη πρέπει να ζητείται πάντα για κάθε διασύνδεση ή περαιτέρω επεξεργασία των προσωπικών του δεδομένων. Επίσης, οι μηχανές αναζήτησης πρέπει να εξετάζουν άμεσα αιτήσεις των χρηστών για διαγραφή στοιχείων που συνεχίζουν να εμφανίζονται στη μνήμη των σελίδων (cache memory) ενώ η σελίδα στην οποία παραπέμπουν έχει πλέον αποσυρθεί. Τέλος, οφείλουν να ενημερώνουν με σαφήνεια τους χρήστες για κάθε πιθανή επεξεργασία των προσωπικών τους δεδομένων και να σέβονται τα δικαιώματα πρόσβασης και αντίρρησης των χρηστών σύμφωνα με το αρ. 12 της Οδηγίας 95/46/ΕΚ.

Επίσης η ομάδα του άρθρου 29 έχει θέσει το ερώτημα, στην οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, αν οι διευθύνσεις IP είναι δεδομένα προσωπικού χαρακτήρα ή όχι. Τονίζεται ότι στις περισσότερες περιπτώσεις, η δυναμική κατανομή διευθύνσεων IP, με τα απαιτούμενα δεδομένα οδηγεί στην αναγνώριση του ή των χρηστών της διεύθυνσης IP αυτό εφαρμόζεται και στις μηχανές αναζήτησης. Η ομάδα εργασίας είχε διευκρινίσει στο WP 136 ότι «… αν οι πάροχοι πρόσβασης στο Διαδίκτυο δεν είναι σε θέση να καθορίσουν με απόλυτη βεβαιότητα ότι τα δεδομένα αντιστοιχούν σε μη ταυτοποιήσιμους χρήστες, θα πρέπει να χειρίζονται όλες τις πληροφορίες IP ως δεδομένα προσωπικού χαρακτήρα για λόγους ασφαλείας …».

4.11 Προτεινόμενες μελλοντικές νομοθετικές τροποποιήσεις

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Πέρα από αυτό, υπάρχουν προτάσεις για τη δημιουργία μιας καινούργιας νομοθεσίας, όπως μια από την Ευρωπαϊκή Επιτροπή που εκδόθηκε το 25/1/2012 – SEC(2012) 73 Final. Η πρόταση αναφέρεται σε μια Ανακοίνωση της Ευρωπαϊκής Ένωσης (COM(2010) 171 Final), στην οποία η Ευρωπαϊκή Επιτροπή σύναψε ότι η Ευρωπαϊκή Ένωση χρειάζεται μια πιο περιεκτική και συνεκτική πολιτική σχετικά με το θεμελιώδες δικαίωμα για προστασία δεδομένων. Το γεγονός ότι αυτή η Ανακοίνωση, που εκδόθηκε στις 20/4/2010, παραδέχεται την έλλειψη κατάλληλης νομοθεσίας σ'αυτό το θέμα, και ότι η πρόταση SEC(2012) 73 Final δεν εκδόθηκε μέχρι δύο χρόνια μετά, δείχνει τις δυσκολίες που αντιμετωπίζει η διαδικτυακή κοινωνία σχετικά με την παραγωγή μιας νομοθεσίας που θα προστατεύει τα δικαιώματα των χρηστών της.

Η πρόταση αυτή έχει ως στόχο (ανάμεσα σε άλλα) το να εξορθολογήσει τη νομοθεσία της Ευρωπαϊκής Ένωσης – γι'αυτό είναι σημαντικό, όπως γράφει στην πρόταση, να φτιαχτεί μια πανευρωπαϊκή νομοθεσία για να υπάρχει ένα κοινό επίπεδο προστασίας σε όλη την Ένωση. Στο κομμάτι 3.2 στην πρόταση, έχει ως εξής – «Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, το οποίο

κατοχυρώνεται στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων, απαιτεί το ίδιο επίπεδο προστασίας των δεδομένων σε ολόκληρη την Ένωση. Η απουσία κοινών κανόνων της ΕΕ ενέχει τον κίνδυνο διαφορετικών επιπέδων προστασίας στα κράτη μέλη και δημιουργεί περιορισμούς στις διασυνοριακές ροές δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών με διαφορετικά πρότυπα.[xlviii]» Συνεχίζει και γράφει – «Οι προτεινόμενες νομοθετικές δράσεις της ΕΕ θα είναι πιο αποτελεσματικές από παρόμοιες δράσεις σε επίπεδο κρατών μελών, λόγω της φύσης και της κλίμακας των προβλημάτων, τα οποία δεν περιορίζονται στο επίπεδο ενός ή μερικών κρατών μελών.»

Η πρόταση περιέχει μία περίληψη σχετικά με του λόγους για τους οποίους υπάρχει. Δηλαδή, έχει μια περιγραφή για τη νομοθεσία που υπάρχει προς στιγμήν, και εξηγεί τις αλλαγές στην κατάσταση του διαδικτύου ώστε να εξηγηθεί η ανάγκη για καινούργια νομοθεσία – «Οι ραγδαίες τεχνολογικές εξελίξεις δημιουργούν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η κλίμακα της ανταλλαγής και της συλλογής δεδομένων έχει αυξηθεί σε μεγάλο βαθμό. Η τεχνολογία επιτρέπει τόσο σε ιδιωτικές επιχειρήσεις όσο και σε δημόσιες αρχές να

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτόγνωρο βαθμό για την επιδίωξη των δραστηριοτήτων τους. Τα φυσικά πρόσωπα καθιστούν ολοένα και περισσότερο δημόσια διαθέσιμες προσωπικές πληροφορίες σε παγκόσμιο επίπεδο. Η τεχνολογία έχει αλλάξει τόσο την οικονομία όσο και την κοινωνική ζωή.[xlix]» Αυτό επιδείχνει την κατανόηση της Κομισιόν ότι είναι δύσκολο για τους νομοθέτες της Ευρωπαϊκής Ένωσης να αντιμετωπίζουν τις γρήγορες αλλαγές στην αγορά που έχουν γίνει παγκοσμίως – ο προηγούμενος νόμος που είχε φτιαχτεί ήταν η απόφαση-πλαίσιο 2008/977/JHA, τέσσερα χρόνια πριν γράφτηκε η πρόταση αυτή, που ήταν απλώς περιείχε κάποιες αλλαγές σχετικά με την προστασία δεδομένων όσον αφορά το δικαστικό σύστημα. Αυτή η απόφαση-πλαίσιο βασικά ορίζει τις ικανότητες των δικαστικών οργανισμών στην Ευρωπαϊκή Ένωση – για παράδειγμα, τα δεδομένα που συλλέγει οποιοσδήποτε δικαστικός οργανισμός μπορούν μόνο να χρησιμοποιούνται για το λόγο που συλλέχθηκαν, αντιθέτως με την ιδιωτική επεξεργασία δεδομένων στην οποία συνήθως μπορεί να χρησιμοποιούνται πληροφορίες για σκοπό διαφορετικό από αυτό για τον οποίον συλλέχθηκαν, εάν δώσει την άδεια για να το κάνουν ο άνθρωπος τον οποίον αφορούν.

Αυτό όμως δεν αποτελεί κάποια μεγάλη αλλαγή στη νομοθεσία που υπάρχει, και βασικά δημιουργήθηκε απλώς για να εξορθολογηστεί η νομοθεσία σε ένα συγκεκριμένο θέμα, δηλαδή το πώς διαχειρίζονται οι πληροφορίες από τα δικαστικά συστήματα. Η πρόταση λοιπόν γράφει και το εξής – «Το ισχύον πλαίσιο παραμένει προσφιλές όσον αφορά τους στόχους και τις αρχές του, αλλά δεν κατάφερε να αποτρέψει τον κατακερματισμό του τρόπου εφαρμογής της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ένωση, την ανασφάλεια δικαίου και μια διαδεδομένη αντίληψη του κοινού ότι υπάρχουν σημαντικοί κίνδυνοι, οι οποίοι σχετίζονται ειδικότερα με την επιγραμμική δραστηριότητα. Για τον λόγο αυτό, πρέπει να οικοδομηθεί ένα ισχυρότερο και πιο συνεκτικό πλαίσιο προστασίας των δεδομένων στην ΕΕ, υποστηριζόμενο από ισχυρή επιβολή του νόμου, η οποία θα επιτρέψει στην ψηφιακή οικονομία να αναπτυχθεί σε ολόκληρη την εσωτερική αγορά, θα επιτρέψει στα φυσικά πρόσωπα να ασκούν έλεγχο επί των δεδομένων που τους αφορούν και θα ενισχύσει τη νομική και την πρακτική ασφάλεια για τους οικονομικούς παράγοντες και τις δημόσιες αρχές.[l]»

Κάτι που πρέπει σε αυτό το σημείο να αναφέρουμε είναι ότι αυτή η πρόταση για αλλαγή νομοθεσίας έγινε μετά από δυο χρόνια έρευνας, η οποία έρευνα περιείχε και

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δύο φάσεις δημόσιας διαβούλευσης, ξεκινώντας το 2009 με μία διάσκεψη υψηλού επιπέδου. Είναι σημαντικό να προσθέσουμε ότι εντός αυτής της περιόδου, έχουν γίνει μέχρι τώρα τέσσερις αλλαγές στην πολιτική ιδιωτικότητας της Google, στις 3/10/2010, στις 20/10/2011, 1/3/2012, και στις 27/7/2012[li]. Αυτό βέβαια επιδείχνει τη διαφορά μεταξύ των ταχυτήτων που λειτουργούν τα συστήματα της αγοράς και τα συστήματα των νομοθετικών θεσμών.

Στην πρόταση γράφει και για ένα συγκεκριμένο λόγο που φτιάχτηκε, ότι υπήρχαν προβλήματα κατακερματισμού δεδομένων – «Διατυπώθηκαν έντονες επικρίσεις για τον παρόντα κατακερματισμό της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ένωση, ιδίως από οικονομικούς παράγοντες οι οποίοι ζήτησαν αύξηση της ασφάλειας δικαίου και εναρμόνιση των κανόνων για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η πολυπλοκότητα των κανόνων για τις διεθνείς διαβιβάσεις δεδομένων προσωπικού χαρακτήρα θεωρείται ότι συνιστά σημαντικό εμπόδιο στις εργασίες τους, καθώς χρειάζονται να διαβιβάζουν τακτικά δεδομένα προσωπικού χαρακτήρα από την ΕΕ σε άλλες περιοχές του κόσμου.[lii]» Είναι ξεκάθαρο ότι η καινούργια νομοθεσία που προτείνεται από την πρόταση αυτή θα υπήρχε σχεδόν μόνο για οικονομικούς λόγους – για να εξορθολογήσει τους κανόνες ώστε οι διεθνείς εταιρείες (δηλαδή, οι «ενδιαφερόμενοι») να είναι πιο σίγουρες όταν λειτουργούν σε δυο ή περισσότερες χώρες της Ένωσης, λογικά για να μειώσουν το κόστος της τήρησης του παρόντος νομικού πλαισίου που εκφράζεται στην οδηγία 95/46/ΕΚ, και τις διάφορες νομοθεσίες που υπάρχουν στα διάφορα κράτη-μέλη.

Εξηγεί μετά κάποιες αλλαγές που αποτελούν διαφορές μεταξύ την παρούσα νομοθεσία και τη νομοθεσία που προτείνεται στο αρχείο. Ένα παράδειγμα είναι το Άρθρο 15, που «Το άρθρο 15 προβλέπει το δικαίωμα πρόσβασης του προσώπου στα δεδομένα προσωπικού χαρακτήρα που το αφορούν, βάσει του άρθρου 12 στοιχείο α) της οδηγίας 95/46/ΕΚ και προσθέτοντας νέα στοιχεία, όπως την ενημέρωση των προσώπων στα οποία αναφέρονται τα δεδομένα για την περίοδο αποθήκευσης και τα δικαιώματα διόρθωσης και διαγραφής καθώς και υποβολής καταγγελίας.[liii]» Αυτό αναφέρεται στην περίοδο της κράτησης των δεδομένων, που σημαίνει ότι αυτό είναι ένα σημαντικό θέμα σχετικά συγκεκριμένα με την παρούσα κατάσταση του διαδικτύου, και το προβλήματα σχετικά με την προστασία δεδομένων που αντιμετωπίζει η Ευρωπαϊκή Ένωση, και ότι δεν θεωρούταν θέμα την περίοδο που φτιαχνόταν η οδηγία 95/46/ΕC.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Άρθρο 9 αναφέρεται στο πως θα επεξεργάζονται ευαίσθητες πληροφορίες όπως τα προαναφερθέντα είδη στο «Safe Harbor», με την πρόσθεση των ειδών όπως το εάν είναι μέλος ενός συνδικάτου, ή εάν έχουν κάποια καταδίκη στο παρελθόν τους. Βέβαια έχει την προϋπόθεση ότι εάν τα δεδομένα έχουν παραδοθεί από τον άνθρωπο στον οποίο αφορούν.

5. Τεχνολογίες για ανώνυμη διαδικτυακή περιήγηση

5.1 Εισαγωγή

Υπάρχουν αρκετές τεχνολογίες ανωνυμοποίησης που έχουν εφαρμοστεί και δοκιμαστεί στην διαδικτυακή περιήγηση. Οι πιο διαδομένες είναι οι mix network(mixnet), crowds, onion routing και tor. Η καλύτερη λύση για μια ασφαλή και ανώνυμη περιήγηση είναι ένα σύστημα ικανό να διασφαλίσει την ιδωτικότητα χωρίς να επηρεάζει την ποιότητα της υπηρεσίας, καθώς πολλές από αυτές έχουν υπολογιστικό κόστος. Αυτό έχει σαν αποτέλεσμα την εμφάνιση καθυστέρησης κατά την διάρκεια της περιήγησης.

5.2 Mixnet

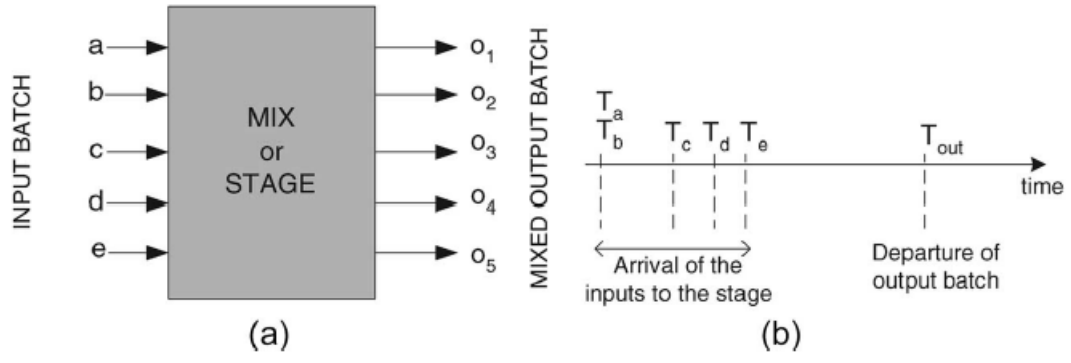
Το 1981, προτάθηκε ένα ανώνυμο κανάλι επικοινωνίας, βασισμένο στην κρυπτογραφία και στην μεταλλαγή το οποίο ονομάστηκε mix networks (mixnet). Το mixnet είναι ένα πολύ-επίπεδο σύστημα που δέχεται ένα σύνολο από εισόδους και παράγει μια έξοδο από σύνολα που περιέχουν την είσοδο κρυπτογραφημένη και μεταλλαγμένη. Η μεταλλαγή και η τυχαία αναδιάταξη της πληροφορίας από το mixnet καθιστά αδύνατη την ανίχνευση της εισόδου από την έξοδο άρα αδύνατη και την αντιστοίχηση μεταξύ εισόδου και εξόδου. Αυτή η ιδιότητα το καθιστά ιδιαίτερα ενδιαφέρον για την επικοινωνία μεταξύ συστημάτων όπου είναι απαραίτητη η ανωνυμία όπως είναι η περιήγηση στο διαδίκτυο[liv].

Ο σχεδιασμός του mixnet έγινε με κεντρικό άξονα τη παροχή ανωνυμίας για ένα σύνολο εισόδων με την αλλαγή της εμφάνισης τους και την αφαίρεση κάθε πληροφορίας σχετικής με την σειρά άφιξης τους. Όπως φαίνεται και στην εικόνα 7 το βασικό στοιχείο του mixnet είναι το ‘stage ή mix’ το οποίο παρέχει την πολυπλεξία των εισόδων. Σημαντικό είναι επίσης ότι η πληροφορία μπορεί να φτάνει σε διαφορετικούς χρόνους όπως φαίνεται και στην εικόνα 7. Η πολυπλεξία συμπεριλαμβάνει την κρυπτογράφηση (κρυπτογράφηση/ αποκρυπτογράφηση) της

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

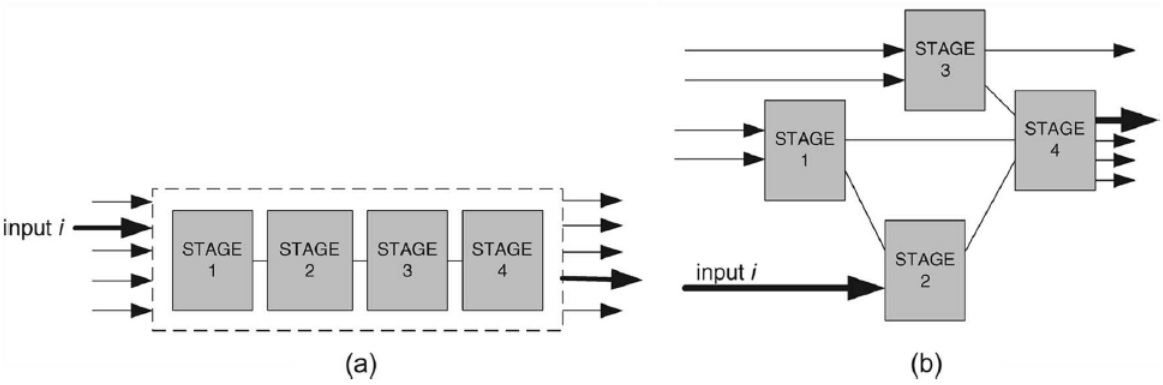
εισόδου και την μεταλλαγή. Η πληροφορία μεταδίδεται στον επόμενο προορισμό σε χρόνο Tout όπως φαίνεται και στην εικόνα 7. Η ομαδοποίηση και η μεταλλαγή της εισόδου έχει σαν αποτέλεσμα να αποκρύβεται η σειρά άφιξης της πληροφορίας. Αν το σύνολο της εισόδου είναι l παρατηρώντας τότε κάποιος την έξοδο από το stage, μπορεί να μαντέψει την αντίστοιχη είσοδο με πιθανότητα 1/l. Για παράδειγμα στην εικόνα 7 όπου το l=5 στην καλύτερη των περιπτώσεων η πιθανότητα να μαντέψει την είσοδο είναι 1/5. Ως εκ τούτου με την αύξηση των αριθμό των εισόδων αυξάνεται και η δυνατότητα ανωνυμοποίησης του stage. Ένα mixnet αποτελείται από έναν αριθμό διασυνδεδεμένων stage, οποίος εξαρτάται από το πόσο ισχυρή ανωνυμία θέλουμε να έχουμε. Κάθε stage πολυπλέκει το σύνολο των εισόδων του και το προωθεί ως είσοδο στο επόμενο stage. Η διασύνδεση των stage αυτή καθαυτή είναι που καθορίζει την τοπολογία του mixnet, η οποία διακρίνεται σε 'cascade' ή 'free-route' όπως φαίνεται και την εικόνα 8 αντίστοιχα [lv lvi].

Η τοπολογία cascade αποτελείται από διασυνδεδεμένα stages με σταθερό και συνεχή τρόπο . Το πρώτο stage λαμβάνει το σύνολο των εισόδων το πολυπλέκει και το μεταφέρει παράλληλα στο επόμενο stage, το οποίο με την σειρά του επαναλαμβάνει την ίδια διαδικασία έως ότου φτάσει στο τελευταίο stage το οποίο και παρέχει την τελική μη ανιχνεύσιμη έξοδο. Ως εκ τούτου όλες οι είσοδοι ακολουθούν την ίδιο δρόμο.



Εικόνα 7: (a)Η πολυπλεξία από το stage που αλλάζει την εμφάνιση των εισόδων και επίσης αφαιρεί κάθε πληροφορία σχετική με την σειρά άφιξης. (b) Διαφορετικός χρόνος άφιξης των εισόδων στο stage.

Η τοπολογία free-route συμπεριλαμβάνει πολλαπλούς δρόμους ανωνυμοποίησης για κάθε είσοδο. Όπως φαίνεται στην εικόνα 8 το stage 2 → stage 4 είναι ένα μονοπάτι ανωνυμοποίησης. Το stage 2 λαμβάνει την είσοδο i και περιμένει κάποια είσοδο από το stage 1,τα πολυπλέκει και τα προωθεί στο stage 4.



Εικόνα 8: Τοπολογίες του mixnet: a) cascade b) free-route

Στο μοντέλο επικοινωνίας mixnet, πολλαπλοί αποστολείς επικοινωνούν με έναν ή περισσότερους δέκτες. Κάθε αποστολέας μπορεί να επικοινωνεί με έναν ή με πολλούς διαφορετικούς δέκτες όπως στην περίπτωση του ηλεκτρονικού ταχυδρομείου ή με έναν όπως στην περίπτωση της διαδικτυακής περιήγησης. Το mixnet παρέχει ανώνυμη επικοινωνία με την προϋπόθεση ότι δύο ή περισσότεροι χρησιμοποιούν το mixnet (πομπός- δέκτης).

5.2.1Σημεία ευπάθειας

Για να μπορέσει να αξιολογηθεί η ασφάλεια του mixnet, θα πρέπει να αναφερθούν οι πιθανές επιθέσεις, που μπορεί να είναι τόσο παθητικές όσο και ενεργές. Μια συνήθης παθητική επίθεση είναι η ‘επίθεση ανάλυσης κίνησης ’, κατά την οποία καταγράφεται η κίνηση της πληροφορίας μεταξύ των διαφόρων stage και έχει σαν σκοπό την αντιστοίχηση μεταξύ εισόδου και εξόδου και κατ΄ επέκταση την άρση της ανωνυμία που παρέχει από το mixnet[lvii].

Μία ενεργή επίθεση είναι η ‘επίθεση χειραγώγησης’, κατά την οποία καταστρέφονται οι είσοδοι των stages με αποτέλεσμα να πλήττεται η ακεραιότητα του mixnet καθώς και να παρακολουθείται και η διαδρομή των κατεστραμμένων εισόδων. Η επίθεση

χειραγώγησης μπορεί να προκαλέσει διαγραφεί, μετατροπή και καθυστέρηση της μετάδοσης.

5.3 Crowds

Το Crowds επιτρέπει την ανάκτηση πληροφοριών από το διαδίκτυο χωρίς να εκθέτει πληροφορίες της ιδιωτικότητας σε τρίτους. Στόχος του Crowds είναι η ανώνυμη περιήγηση, ούτος ώστε είτε η πληροφορία που αφορά τον χρήστη, είτε η πληροφορία που ανακτάται από το δίκτυο, να παραμένει κρυφή από άλλους.

Το Crowds εξασφαλίζει την μη καταγραφή πληροφοριών από τους εξυπηρέτες, όπως η IP και το domain, οι οποίες μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του χρήστη. Επίσης, είναι δυνατό να διασφαλίσει το απόρρητο σε πληροφορίες όπως τη ιστοσελίδα από την οποία προήλθε ο χρήστης και τον τύπο υπολογιστή του χρήστη, καθώς και να αποκρύψει πληροφορίες σε όσους θα μπορούσαν να καταγράφουν απευθείας τα μηνύματα από τον υπολογιστή του χρήστη.

Το Crowds βασίζεται στο ότι κάποιος μπορεί να εξασφαλίσει την ανωνυμία του όταν βρίσκεται μέσα στο πλήθος. Έτσι, αντί να υπάρχουν HTTP αιτήσεις μέσω ενός δρομολογητή, πραγματοποιούνται δια μέσω ενός πλήθους (crowd): το πλήθος που δημιουργείται από τους πελάτες , χωρίς να λαμβάνεται υπόψη η γεωγραφική θέση, πραγματοποιεί τις συναλλαγές στο διαδίκτυο εκ μέρους των μελών του. Για να γίνει κάποιος μέλος στο πλήθος, χρησιμοποιεί μία Jondo διεργασία, που υποδηλώνει ένα τυχαίο και ανώνυμο πρόσωπο μέσα στο πλήθος. Κατ' επέκταση, ο κάθε χρήστης μέσα στο πλήθος αντιπροσωπεύεται από το Jondo που εκτελείται στον υπολογιστή του [lviii].

Όταν ξεκίνα η Jondo διαδικασία εδραιώνεται μία επικοινωνία με το Onion routing πλήθος μέσω ενός πρωτοκόλλου. Αυτό ενημερώνει τα υπόλοιπα μέλη του πλήθους για τη νέο μέλος, όσο και το ίδιο για τα υπόλοιπα μέλη. Ο χρήστης για να πραγματοποιήσει αιτήσεις στο διαδίκτυο πρέπει να προβεί σε κάποιες ρυθμίσεις στο φυλλομετρητή του. Πρέπει να ορίσει αυτή ως κύριο εξυπηρετητή για όλες τις δικτυακές του εφαρμογές. Έτσι, όταν δεχτεί μία αίτηση από το φυλλομετρητή, η

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Jondo διαδικασία επιλέγει τυχαία κάποιον από το πλήθος και του αποστέλλει την αίτηση.

Όταν ο χρήστης προσπαθήσει να επισκεφτεί κάποια σελίδα μέσου του φυλλομετρητή του, η αίτηση θα αποσταλεί στη Jondo και όχι στον άμεσο-εξυπηρετητή της σελίδας. Η πιθανότητα για μία αίτηση να προωθηθεί ξανά σε κάποιον μέσα στο πλήθος, παρά να προωθεί άμεσα στον εξυπηρετητή, είναι περισσότερο από 0.5 [lix]. Οι αιτήσεις του χρήστη με ένα τυχαίο τρόπο καταλήγουν σε ένα μέλος. Είναι αδύνατη η σύνδεση μεταξύ αίτησης και χρήστη ακόμη και από τον μέσω του proxy.

Ακόμη, υπάρχει η δυνατότητα για επιπλέον προστασία από την άμεση παρακολούθηση των μηνυμάτων που ανταλλάσει ο υπολογιστής του χρήστη. Πιο συγκεκριμένα, η Crowds τοπολογία μπορεί να αποκρύψει τις σελίδες που επισκέπτεται ο χρήστης τόσο από τρίτους αλλά όσο και από τα υπόλοιπα μέλη τους πλήθους, τα οποία χρησιμοποιεί για να μπορέσει να συνδεθεί. Η επικοινωνία μεταξύ Jondos κρυπτογραφείται συμμετρικά μέσω κλειδιού το οποίο διαμοιράζεται από πριν.

5.3.1 Αρχές Λειτουργίας

Στο πρωτόκολλο Crowds η δημιουργία του μονοπατιού μεταξύ των proxies γίνεται τυχαία καθώς η αίτηση από τον χρήστη προχωράει ανάμεσα στα μέλη. Το μονοπάτι το οποίο δημιουργείται χρησιμοποιείται για όλες τις ανώνυμες αιτήσεις του χρήστη, που συχνά καλείται και ως ιδρυτής εικόνα 9. Το Crowds αφού αρχικοποιήσει, κάνει γνωστό στον αποστολέα ένα κλειδί το οποίο είναι γνωρίζουν και τα υπόλοιπα μέλη μέσω του Jondo [lx lxi] . Ο ιδρυτής για να αποστείλει δεδομένα, δημιουργεί και προωθεί ένα πακέτο, στο συμπεριλαμβάνεται το τυχαίο μονοπάτι, η IP του δέκτη (R), και τέλος τα δεδομένα κρυπτογραφημένα, το οποίο είναι γνωστό και στο επόμενο επιλεγμένο μέλος.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

I→j: {R, p, data}KIj[8]

Το Pf ($0.5 \leq Pf \leq 1$) είναι αυτό που καθορίζει κατά πόσο το πακέτο με ένα id θα προωθηθεί στον τελικό δέκτη ή θα προωθηθεί σε ένα τυχαία Jondo.

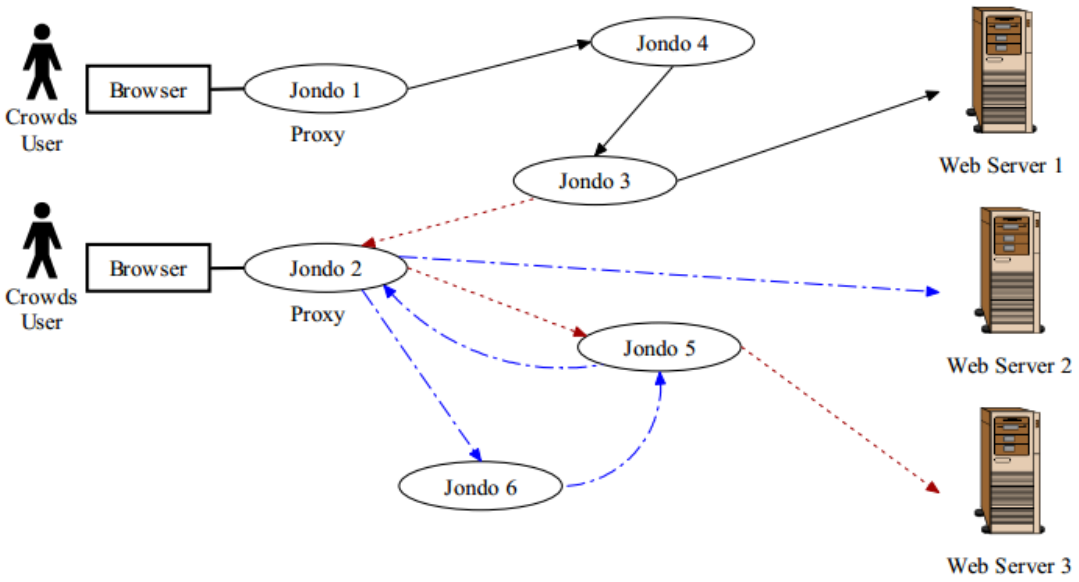
j΄ →R : p΄΄, data

Όταν ο δέκτης παραλάβει το πακέτο, απαντάει ένα πακέτο ότι το έλαβε ακολουθώντας την αντίθετη διαδρομή του μονοπατιού. Όλα τα πακέτα μετά την πρώτη επικοινωνία μεταξύ αποστολέα και παραλήπτη θα ακολουθήσουν την ίδια διαδρομή. Ο ιδρυτής είναι προφανές ότι υπάρχει σε κάθε μονοπάτι[lxii].

Το Crowds μπορεί να αλλάζει τα μονοπάτια κάθε 24 ώρες, έτσι ώστε να μειωθεί ο αριθμός των διαθέσιμων μονοπατιών. Αυτή η στατικότητα των μονοπατιών για 24 ώρες μπορεί να δημιουργήσει άλλα προβλήματα όπως να αναγνωρίζονται άμεσα τα όλα τα νέα μέλη στο πλήθος καθώς όλα τα παλαιότερα θα έχουν εδραιώσει ήδη κάποιο μονοπάτι.

[8] Κλειδί κρυπτογράφησης

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Εικόνα 9: Μονοπάτια σε ένα Crowd. Ο αριθμός του Jondo υποδεικνύει το χρήστη που πραγματοποιεί την αίτηση και τον εξυπηρετητή ιστού που απευθύνεται.

Καθόλη την διάρκεια που ταυτότητες των μελών είναι γνωστές και δημόσιες, οι παραλήπτες αλλά και οι τρίτες οντότητες δεν είναι ενήμεροι για τον ιδρυτή, καθώς δεν μπορούν να γνωρίζουν αν είναι αυτός ή είναι ένα μέλος του μονοπατιού που προωθεί το μήνυμα. [lxiii].

5.3.1 Σημεία ευπάθειας

Επειδή κάθε μέλος του μονοπατιού μπορεί να αιτηθεί τερματισμό της σύνδεσης, ο εξυπηρετητής καταγράφει σε λίστα την IP του αιτηθέντος ως την διεύθυνση του αρχικού αιτούντος.

Παρόλο που το Crowds παρέχει μια επαρκή ανωνυμία για τον αιτούμενο, δεν προστατεύεται η ακεραιότητα του περιεχομένου των αιτήσεων μεταξύ των Jondos κατά την διάρκεια του μονοπατιού. Τελικά το θέμα αυτό λύθηκε με κρυπτογράφηση στην end to end επικοινωνία μεταξύ χρήστη και εξυπηρετητή.

Όπως σε κάθε ανώνυμη υπηρεσία βασισμένη μπορεί να παρακαμφθεί εάν ο φυλλομετρητής του χρήστη ανακτά και εκτελεί κινητό κώδικα ώστε να εδραιώνει μια

σύνδεση με τον εξυπηρετητή. Τέλος ένα άλλο μειονέκτημα του Crowds είναι ότι αυξάνει την κίνηση του δικτύου και επιβαρύνει τους κόμβους.

5.3 Onion routing

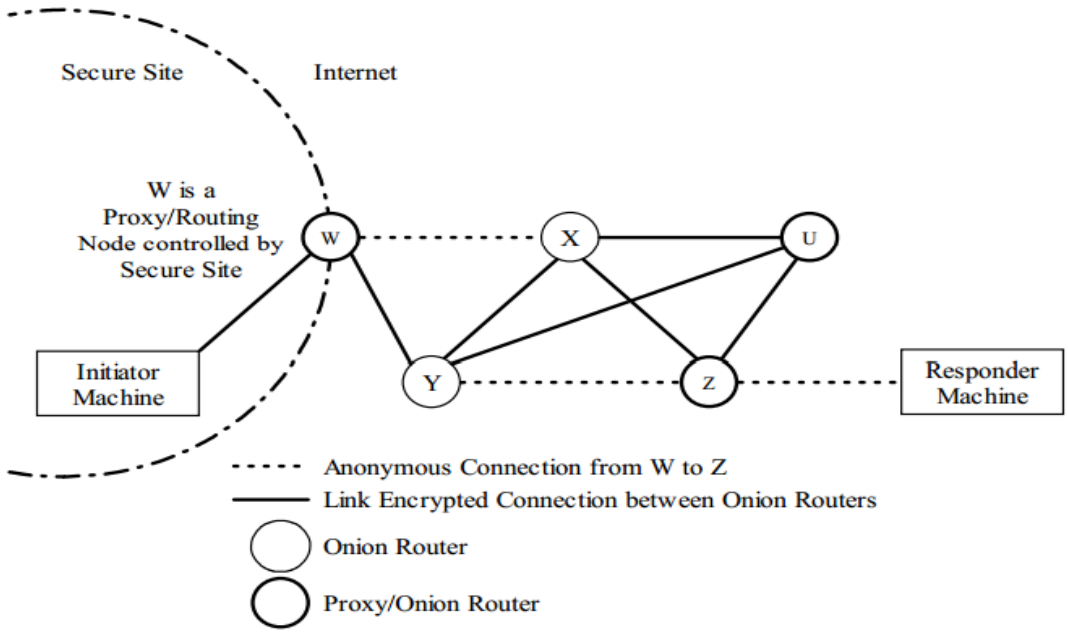
Μια ακόμα τεχνολογία για ανώνυμη περιήγησης στον παγκόσμιο ιστό είναι και Το Onion Routing. Με αυτή την τεχνολογία μπορούμε να επιτύχουμε, μέσο διαφορετικών επιπέδων κρυπτογράφησης ανώνυμες συνδέσεις. Οι συνδέσεις αυτές μπορεί να είναι είτε προσανατολισμένες είτε άνευ εγκατάστασης και μάλιστα χαρακτηρίζονται πολύ ισχυρές έναντι επιθέσεων.

Η γενική ιδέα αυτής της τεχνολογίας είναι το να αναμιγνύει ουσιαστικά τις συνδέσεις και τις εφαρμογές των χρηστών ώστε να μην είναι δυνατή η ταύτιση ενός χρήστη [lxiv].

Η δομή της onion δρομολόγησης είναι από δύο μέρη : την υποδομή δικτύου και τους πληρεξούσιους. Η υποδομή δικτύου χρησιμοποιείται για τις ανώνυμες συνδέσεις και επίσης περιέχει και τους onion δρομολογητές. Οι δρομολογητές Onion όταν συνδεθούν στο παγκόσμιο ιστό μπορούν να επικοινωνήσουν επειδή έχουν, μόνο μία, σύνδεση με τους γειτονικούς δρομολογητές onion. Το δεύτερο κομμάτι είναι οι πληρεξούσιοι που χρειάζονται για την σύνδεση των εφαρμογών του χρήστη και κάθε μία σύνδεση στο παγκόσμιο ιστό. Έτσι οι πληρεξούσιοι είναι υπεύθυνοι για την μετάφραση των δεδομένων σε άλλη μορφή, διαφορετική από την αρχική, ώστε να γίνεται αντιληπτή από τους Onion δρομολογητές.

Οι δρομολογητές μπορούν να γνωρίζουν και τα δημόσια κλειδιά των των άλλων δρομολογητών καθώς και την ταυτότητά τους. Ο αποστολέας από την πλευρά του έχει ένα πληρεξούσιο ο οποίος είναι και αυτός που θα κάνει την επιλογή της διαδρομής . Σε όλη την διαδρομή θα συναντάει και άλλους δρομολογητές από τους οποίους θα κάνει συλλογή κάποιων στοιχείων (την ip και όλα τα αναγκαία στοιχεία για την αναπαραγωγή του κλειδιού κρυπτογράφησης), ώστε να μπορεί να συνεχίσει την διαδρομή του. Έτσι δημιουργείται το Onion δηλαδή η διαδρομή για την σύνδεση με τον παγκόσμιο ιστό εικόνα 10 [lxv].

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Εικόνα 10: Παράδειγμα δικτύου Onion Routing με μία ανώνυμη σύνδεση από έναν ιδρυτή σε ένα ανταποκριτή διαμέσου των δρομολογητών W, X, Y και Z.

Όπως προαναφέρθηκε είναι υπεύθυνοι για την μετάφραση των δεδομένων σε άλλη μορφή αλλά μία ακόμα λειτουργία τους είναι και να λειτουργούν και σαν ενδιάμεσοι δρομολογητές ώστε να μην μπορεί να δημιουργηθεί κανένας συμψηφισμός πληροφοριών και άρα κάποια εξαγωγή συμπερασμάτων. Έτσι όταν αρχίζει η διαδικασία η πρώτη προσπέλαση πρέπει να γίνει σε κάποιον Onion . Εδώ βέβαια υπάρχουν διαφορετικές περιπτώσεις όπως το που γίνεται η εκτέλεση του πληρεξουσίου . Υπάρχουν οι περιπτώσεις το να εκτελείται τοπικά και μη τοπικά. Όταν η εκτέλεση είναι τοπική το υπολογιστικό κόστος είναι μεγαλύτερο σε σχέση με το να εκτελείται μη τοπικά που έχουμε κρυπτογραφημένη σύνδεση και το κόστος είναι μηδέν.

Από τα παραπάνω γίνεται αντιληπτό ότι ένας πληρεξούσιος είναι το τμήμα που αντικαταστεί μέσω διεπαφών (socket), μεταξύ των εφαρμογών και των συνδέσεων, τις συνδέσεις tcp και ip [lxvi].

Εδώ θα πρέπει να αναφέρουμε και τα τρία τμήματα του πληρεξούσιου που είναι τα εξής: Το μη απαραίτητο και το ειδικευμένο φίλτρο και τον πληρεξούσιο. Το Πρώτο φίλτρο χρησιμοποιείται για την διαμόρφωση των ποών. Το Ειδικευμένο μετατρέπει τις ροές από την αρχική τους μορφή σε μια συμβατή με το Onion σύστημα. Τέλος το

πληρεξούσιο το οποίο ουσιαστικά κατευθύνει τις συνδέσεις αλλά για αυτό θα πρέπει να γνωρίζει και την τοπολογία του δικτύου και τα δημόσια κλειδιά.

Εν συνεχεία θα πρέπει να γίνει μία αναφορά στις διεπαφές στα είδη των διεπαφών τα οποία δημιουργούνται τα οποία είναι μεταξύ του της μεριάς του αποστολέα και του πληρεξουσίου. Μετά ακολουθεί η ανώνυμη σύνδεση η οποία επικοινωνεί και με τους τρείς δηλαδή τον αποστολέα τον πληρεξούσιο και τον τελικό παραλήπτη. Τέλος υπάρχει η διασύνδεση μεταξύ του πληρεξουσίου (το οποίο είναι στον τελικό παραλήπτη και στον ίδιο τον παραλήπτη). Όλα αυτά λειτουργούν αμφίδρομα.

Για να περιγράψουμε την διαδρομή ανάμεσα στους δρομολογητές έχουμε σαν βασική αρχή την γνώση ότι τα δημόσια κλειδιά και η ταυτότητες είναι γνωστές για όλους τους δρομολογητές. Για την περιγραφή της λειτουργίας του Onion Routing θεωρείται ότι κάθε Onion δρομολογητής γνωρίζει τις ταυτότητες και τα δημόσια κλειδιά κάθε άλλου δρομολογητή Onion. Έτσι όταν ο αρχικός δρομολογητής ξεκινάει να μία διαδρομή τότε για να μεταβεί στον επόμενο δημιουργεί ένα πακέτο το οποίο περιέχει την διεύθυνση του επόμενου, το κρυπτογραφημένο κλειδί καθώς και τον επόμενο επίπεδο που θα πρέπει να μετακινηθεί. Στο εσωτερικό επίπεδο των Onion υπάρχουν τα δεδομένα που είναι για αποστολή και την ταυτότητα του ανταποκριτή.

Τα επίπεδα είναι κρυπτογραφημένα από το δημόσιο κλειδί του παραλήπτη δρομολογητή. Κάθε ζευγάρι των δρομολογητών για να μην χρειαστεί σε μια μελλοντική σύνδεση η αποστολή ενός επιπλέον Onion δημιουργεί ένα αναγνωριστικό της τοπικής σύνδεσης (aci).

Έτσι δημιουργείται ένα μονοπάτι ανάμεσα στον αποστολέα και τον παραλήπτη δρομολογητή που είναι το ίδιο κάθε φορά, το οποίο λειτουργεί αντίστοιχα και αμφίδρομα [lxvii].

Ένα ακόμα χαρακτηριστικό για την ενίσχυση της ασφάλειας είναι ότι η λογική της onion δρομολόγησης στηρίζεται σε chaum mixes με την οποία τα μηνύματα που αποστέλλονται ενώ είναι σταθερά σε μέγεθος αποστέλλονται με τυχαίους συνδυασμούς και από διαφορετικές πηγές μαζικά, με αποτέλεσμα να μην μπορεί να γίνει αντιστοίχηση αυτών και του χρήστη. Στο δίκτυο του Onion Routing επειδή μπορεί να περιγραφεί σαν κατανεμημένο έχει ανοχή σε σφάλματα. Και για αυτό τον

λόγο ένας μόνο δρομολογητής Onion δεν είναι δυνατό να καταρρίψει το δίκτυο, ούτε μπορεί να παραβιάσει την ανωνυμία ενός χρήστη.

Αναφορικά με τις συνδέσεις του που έχουμε με αυτή την μέθοδο μπορούν να διαχωριστούν σε τρία τμήματα.

Στην πρώτο τμήματα , αφού έχουμε και το onion, σχεδιάζεται η διαδρομή και επιλέγονται τα κλειδιά. Η πρώτη φάση ξεκινά όταν ο χρήστης δημιουργήσει ένα Onion και τότε καθορίζεται το μονοπάτι του δικτύου που θα ακολουθήσει η σύνδεση. Στην επόμενη φάση γίνεται η αποκρυπτογράφηση του onion και τελικά τα δεδομένα στέλνονται και στον αποστολέα αλλά και στον παραλήπτη. Η τελική φάση είναι όταν παύει να υπάρχει η onion δρομολόγηση. Εδώ θα πρέπει να αναφερθεί ότι τα δεδομένα που υπάρχουν στους δρομολογητές για την διαδρομή διαγράφονται αυτόματα μετά την λήξη της δρομολόγησης [lxviii].

.

5.3.1 Σημεία Ευπάθειας

Η τεχνολογία Onion Routing δεν είναι απρόσβλητη σε επιθέσεις ανάλυσης κίνησης. Εάν υπάρχει κάποια εφαρμογή εκφραζόμενη από αιτήσεις δικτύου που απαιτεί σύνδεση πραγματικού χρόνου, είναι πιθανή η ανίχνευση της ταυτόχρονης εισόδου των πλησιέστερων συνδέσεων socket των Onion routing πληρεξούσιων του ιδρυτή και του ανταποκριτή. Ωστόσο, αυτές οι μορφές επιθέσεων απαιτούν τη συλλογή και ανάλυση τεράστιων ποσών δεδομένων από εξωτερικούς παρατηρητές.

5.5 Tor

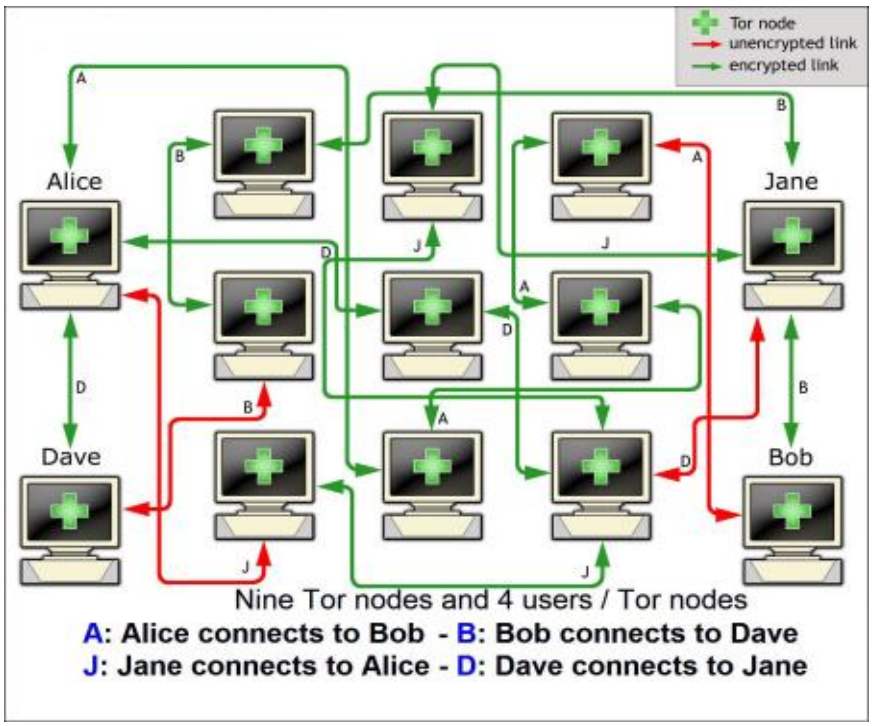
Το Tor δίκτυο είναι βασισμένο στο onion-routing όπως αυτό, παρουσιάστηκε παραπάνω, όπου η κίνηση προωθείτε μέσω πολλαπλών δρομολογητών κρυπτογραφημένη. Το μονοπάτι μέσα στο δίκτυο είναι έτσι φτιαγμένο ούτως ώστε κάθε δρομολογητής να γνωρίζει μόνο τον προηγούμενο και τον επόμενο. Στην πραγματικότητα ο πρώτος δρομολογητής γνωρίζει την πηγή της πληροφορίας και ο τελευταίος τον προορισμό. Παρόλαυτά, αν και οι δυο αυτοί δρομολογητές

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συνεργαστούν, μπορούν να εκτιμήσουν την κίνηση της πληροφορίας. Οι tor δρομολογητές εγγράφονται σε μία λίστα. Κάθε δρομολογητής αναφέρει την IP του, το δημόσιο κλειδί του, την πολική που θα ακολουθήσει σε σχέση με την κίνηση που θα δεχτεί και σε ποια ταχύτητα. Επίσης μέσω αυτής της λίστας παρέχεται και ο χρόνος αδιάλειπτης λειτουργίας του κάθε δρομολογητή. Ο αλγόριθμος tor (για την δημιουργία του μονοπατιού) εκτελείται από τον tor - πελάτη αφού διαλέξει πρώτα όλους του διαθέσιμους δρομολογητές εικόνα 11. Μετέπειτα επιλέγεται από το tor-πελάτη ψευδοτυχαία (λαμβάνεται υπόψη το εύρος ζώνης) ένας δρομολογητής . Με αυτόν τον τρόπο το εύρος ζώνης είναι σχετικά ισορροπημένο μεταξύ των tor-κόμβων σε αναλογία με το εύρος ζώνης που έχουν στη διάθεσή τους [lxix]. Για την αποφυγή αδικαιολόγητης υψηλής αναφοράς σε εύρος ζώνης από κάποιο δρομολογητή έχει οριστεί ως άνω όριο το 1.5MBs. Το tor πρωτόκολλο περιλαμβάνει τα ακόλουθα:

Άριστη και άμεση εμπιστευτικότητα: Στο γνήσιο Onion-Routing σχεδιασμό, ένας εχθρικός κόμβος μπορούσε να καταγράψει την κίνηση της πληροφορίας και στην συνέχεια να θέση σε κίνδυνο διαδοχικούς κόμβους στο κύκλωμα και να τους αναγκάσει να την αποκρυπτογραφήσουν. Το tor αντί μίας πολλαπλά κρυπτογραφημένης δομής δεδομένων (ένα onion), χρησιμοποιεί ένα επαυξητικό ή τηλεσκοπικό σχεδιασμό, στο οποίο ο tor πελάτης διαπραγματεύεται με κλειδιά συνεδρίας κάθε μεταπήδηση μέσα στο κύκλωμα του tor. Καθώς αυτά τα κλειδιά καταστρέφονται, καθίσταται αδύνατο από τους κόμβους να αποκρυπτογραφηθεί παλαιότερη κίνηση .

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Εικόνα 11: λειτουργία του TOR

Διαχωρισμός "πρωτόκολλο καθαρισμού" από την ανωνυμία: Το tor χρησιμοποιεί τις σχεδόν μοναδικές SOCKS proxy διεπαφές, με αποτέλεσμα να υποστηρίζει περισσότερες εφαρμογές- TCP χωρίς καμία περαιτέρω αλλαγή.

Όχι 'mixing, padding, και traffic shaping': Προς το παρόν το tor δεν χρησιμοποιεί mixing, padding ούτε και traffic shaping που στο onion routing έχουν αναλυθεί εκτενώς και χαρακτηριστεί ως μη πρακτικά και ασύμφορα (ως προς το υπολογιστικό κόστος) .

Πολλαπλές TCP ροές μπορούν να διαμοιραστούν στο ίδιο κύκλωμα: Το Onion routing χρησιμοποιεί ξεχωριστό κύκλωμα για κάθε απαίτηση-εφαρμογής, το οποίο απαιτεί πολλαπλά δημόσια κλειδιά για κάθε μία αίτηση. Επίσης η δημιουργία τόσων κυκλωμάτων εγείρει πιθανές απειλές για την ανωνυμία του χρήστη. Το tor με την πολυπλεξία των TCP ροών για κάθε κύκλωμα βελτιώνει την αποτελεσματικότητα και την ανωνυμία.

5.6 Τεχνολογικές προτάσεις για καλύτερη διαχείριση των πληροφοριών ώστε να είναι χρηστικές αλλά και λιγότερο επικίνδυνες

Η επικρατέστερη τεχνολογία για μια ανώνυμη περιήγηση στον παγκόσμιο ιστό και οι περισσότερες έρευνες σε τέτοιου είδους τεχνολογίες αναφέρονται στην ανάπτυξη νέων και ποιο βελτιωμένων τρόπων λειτουργίας των Tor. Η αρχιτεκτονική που θα αναφερθεί παρακάτω [lxx] θεωρείτε η επικρατέστερη και οι βασικοί της στόχοι είναι να επιτύχει τα εξής:

1. Επεκτάσιμη αρχιτεκτονική: Η σχεδίαση του νέου συστήματος θα έχει σαν πρωταρχικό στόχο ένα σχέδιο για ανώνυμη επικοινωνία που να είναι σε θέση να αναβαθμίσει τον αριθμό των συνεργατών και των πελατών του δικτύου, θα βελτιώνει την απόδοση του δικτύου και επίσης θα αυξάνει την ανωνυμία των χρηστών.

2. Ασφάλεια: Οι μέχρι τώρα εργασίες για τις κλιμακούμενες ανώνυμες επικοινωνίες παρέχουν μόνο ευρετικές εγγυήσεις για την ασφάλεια. Στόχος της παρούσας πρότασης είναι ένας σχεδιασμός που αξιοποιεί πλήρως τους μηχανισμούς ασφαλείας και που κατ' επέκταση καθιστά σχετικά εύκολο να αναλυθεί η ασφάλεια του συστήματος. Επίσης στόχος είναι να επιτευχθούν παρόμοιες ιδιότητες ασφαλείας όπως και στο υπάρχον δίκτυο Tor. Είναι γνωστό ότι λογικές παραμέτρους του Private information retrieval- Tor (PIR-Tor) [lxxi] είναι σε θέση να παρέχουν ισοδύναμη ασφάλεια με το δίκτυο Tor.

3. Αποδοτική δημιουργία κυκλώματος: αρχιτεκτονικές που επιβάλλουν επιπλέον καθυστέρηση κατά τη διάρκεια της δημιουργίας του κυκλώματος μπορεί να μην είναι πρακτικές, δεδομένου ότι ο χρήστης θα πρέπει να περιμένει για τη δημιουργία κυκλώματος να ολοκληρωθεί πριν από την έναρξη της ανώνυμης επικοινωνίας.

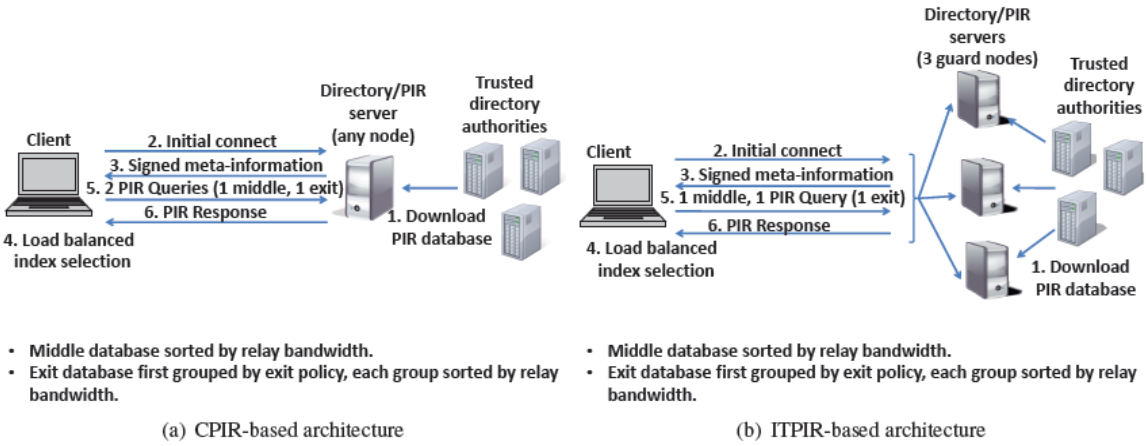
4. Διατήρηση των περιορισμών Tor: Το δίκτυο Tor επιβάλλει διάφορους περιορισμούς σχετικά με την επιλογή των συνεργατών κατά την κατασκευή του κυκλώματος. Για παράδειγμα, ο πρώτος συνεργάτης θα πρέπει να είναι ένας από τους φρουρούς του χρήστη, ενώ ο τελικός θα πρέπει να επιτρέπει την έξοδο της πληροφορίας στην επιθυμητή θύρα του χρήστη, καθώς και γενικότερα οι συνεργάτες θα πρέπει να επιλέγονται ανάλογα με το εύρος ζώνης τους, έτσι ώστε να επιτυγχάνεται η εξισορρόπηση του φορτίου του δικτύου.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Η Αρχιτεκτονική του συστήματος.

Οι βασικές γνώσεις μας κατά το σχεδιασμό PIR-Tor είναι ότι το μοντέλο client-server σε Tor μπορεί να διατηρηθεί, ενώ ταυτόχρονα βελτιώνει την επεκτασιμότητα του, έχοντας τους χρήστες να κατεβάζουν τις περιγραφές λίγων μόνο επαφών του συστήματος, σε αντίθεση με τη λήψη της συνολικής εικόνας. Ωστόσο, αφελώς με αυτόν τον τρόπο μπορεί να επιτραπεί σε κακόβουλους διακομιστές καταλόγου να εξαπολύσουν 'fingerprinting' επιθέσεις κατά των των χρηστών, με αποτέλεσμα να τίθεται σε κίνδυνο η ανωνυμία. Έτσι προτείνετε στους χρήστες να αξιοποιούν τα ιδιωτικά πρωτόκολλα ανάκτησης πληροφοριών για να κατεβάζουν τις ταυτότητες ορισμένων συνεργατών, ώστε να επιτυγχάνεται η προστασία της ιδιωτικότητας κατά κακόβουλων διακομιστών. Επειδή ο πελάτης δεν χρειάζεται να χρησιμοποιεί ένα πρωτόκολλο PIR για να επιλέξει το κάθε φύλακα συνεργάτη. Μια πλήρη λήψη του δικτύου συνεργατών και τις περιγραφές τους αρκεί , αφού η επιλογή του συνεργάτη φύλακα είναι μια one-time λειτουργία, που δεν επηρεάζει την επεκτασιμότητα του πρωτοκόλλου.

Επίσης η ιδιωτική ανάκτηση πληροφοριών έχει δύο αποκλίνουσες: computational PIR και Information-theoretic PIR. Ενώ και οι δύο, computational PIR (CPIR), information-theoretic PIR (ITPIR), μπορούν να χρησιμοποιηθούν από τους πελάτες, οι υποκείμενες τεχνικές έχουν διαφορετικά μοντέλα απειλής, με αποτέλεσμα να υπάρχουν ελαφρώς διαφορετικές αρχιτεκτονικές, όπως απεικονίζεται στην εικόνα 12.



Εικόνα 12: Αρχιτεκτονική συστήματος: Για την CPIR αρχιτεκτονική, επιλέγεται ένα αυθαίρετο σετ από συνεργάτες (PIR διακομιστές) που διατηρούν ένα τρέχων αντίγραφο της PIR βάσης καθώς στην ITPIR αρχιτεκτονική οι φύλακες συνεργάτες είναι οι διακομιστές καταλόγου. Αυτοί κατεβάζουν την PIR βάση από μία έμπιστη

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

αρχή. Έπειτα πραγματοποιείται μία PIR ερώτηση, κατά την οποία οι χρήστες πρώτα λαμβάνουν μετα-πληροφορίες για την PIR βάση από τους διακομιστές καταλόγου και μετέπειτα χρησιμοποιούν αυτές για να εντοπίσουν το συγκεκριμένα τμήμα που αφορά την πληροφορία. Πάντα λαμβάνεται υπόψη το εύρο ζώνης και την πολιτική εξόδου των συνεργατών. Πληροφορίες συνεργατών μπορούν να χρησιμοποιούν για την εδραίωση ανώνυμης επικοινωνίας.

Computational PIR σε διακομιστές καταλόγου: Η computational PIR μπορεί να εγγυηθεί την προστασία της ιδιωτικότητας των χρηστών, ακόμη και όταν υπάρχει μια ενιαία αξιόπιστη βάση δεδομένων. Σε αυτό το σενάριο, προτείνεται ότι κατά την τρέχουσα αρχιτεκτονική Tor, κάθε συνεργάτης μπορεί να λειτουργήσει ως ένας διακομιστής καταλόγου. Οι διακομιστές καταλόγου διατηρούν μια συνολική εικόνα του συστήματος, και λειτουργούν ως βάση δεδομένων PIR. Οι πελάτες μπορούν να χρησιμοποιήσουν στη συνέχεια ένα πρωτόκολλο CPIR ώστε να υποβάλουν ερωτήματα στους διακομιστές καταλόγου και να λάβουν τις ταυτότητες των τυχαίων επαφών στο σύστημα. Information-theoretic PIR σε αρχές κατάλογου (απορρίφθηκε): Η Information-theoretic PIR μπορεί να εγγυηθεί την προστασία της ιδιωτικότητας των χρηστών μόνο όταν ένας οριακός αριθμός των βάσεων δεδομένων δεν συνωμοτούν. Από τη στιγμή που διακομιστές καταλόγου στο τρέχον δίκτυο Tor είναι αναξιόπιστοι, δεν μπορούν να χρησιμοποιηθούν ως PIR βάσεις δεδομένων. Ωστόσο, το Tor έχει οκτώ αρχές καταλόγων που υπογράφουν τη συνολική εικόνα του συστήματος (η συναίνεση του δικτύου).

Εφόσων το Tor εμπιστεύεται ήδη ότι η πλειοψηφία του καταλόγου αρχές είναι ειλικρινείς, μια πιθανή λύση που θα μπορούσε να έχει ήταν να χρησιμοποιήσει τις αρχές καταλόγου με PIR βάσεις δεδομένων. Ωστόσο, η προσέγγιση αυτή απορρίπτεται, δεδομένου ότι οι αρχές κατάλογου θα δημιουργήσει προβλήματα στην απόδοση στο σύστημα, και θα γίνει στόχος DDoS επιθέσεων.

Information-theoretic PIR στο συνεργάτη φύλακα: Αντ 'αυτού, αναφέρεται ότι το Tor δείχνει εμπιστοσύνη στους φύλακες κόμβους. Αν όλοι οι συνεργάτες φύλακες του πελάτη είναι σε κίνδυνο, τότε μπορεί να εκτελεστεί μία από άκρο-σε-άκρο ανάλυση χρονισμού σε συνδυασμό με DOS επιθέσεις και να σπάσει την ανωνυμία των χρηστών στο υπάρχων δίκτυο Tor. Έτσι θεωρείτε ότι ο πελάτης χρησιμοποιεί τρεις κόμβους φρουράς για διακομιστές του ITPIR. Μέχρι και οι τρεις κόμβοι φρουράς, δεν είναι σε κίνδυνο δεν μπορεί να μαθευτεί η ταυτότητα των συνεργατών που έχουν

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κατέβει από τους πελάτες. Ακόμα κι αν και οι τρεις ρελέ φύλακες είναι σε κίνδυνο, δεν μπορούν να χειριστούν ενεργά στοιχεία της βάσης δεδομένων PIR, δεδομένου ότι έχουν υπογραφεί από το αρχές καταλόγου, μπορούν μόνο να μάθουν τις περιγραφές των συνεργατών εξόδου που είχαν κατέβει από τους πελάτες. (Στην Tor τοπολογία, οι φύλακες συνεργάτες γνωρίζουν πάντα την ταυτότητα των ενδιάμεσων κόμβων μέσα στο κύκλωμα) Εάν ο συνεργάτης εξόδου σε ένα κύκλωμα είναι ειλικρινής, τότε ο συνεργάτης φύλακας δεν μπορεί να σπάσει την ανωνυμία των χρηστών. Από την άλλη πλευρά, εάν ο συνεργάτης εξόδου που χρησιμοποιείται είναι κακόβουλος, τότε η ανωνυμία των χρηστών έχει σπάσει , αλλά σε αυτό το σενάριο, θα μπορούσε να έχει πραγματοποιηθεί ούτως ή άλλως μία άκρο-σε-άκρο ανάλυση χρονισμού (στο τρέχον δίκτυο Tor)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

6. Συμπεράσματα και επίλογος

Οι μηχανές αναζήτησης, στην σύγχρονη εποχή, αποτελούν ένα πολύ χρήσιμο εργαλείο για την περιήγηση στον παγκόσμιο ιστό. Τα προβλήματα όμως που προκύπτουν για την ιδιωτικότητα απασχολούν όλο και περισσότερες ομάδες ανθρώπων.

Η ευθύνη της διατήρησης της ιδιωτικότητας θα μπορούσε να ξεκινάει από τον ίδιο τον χρήστη με τις ενέργειές του, όπως για παράδειγμα την απενεργοποίηση κάποιων cookies η με την άρνησή του σε πολιτικές που ακολουθούν κάποιες εταιρείες που διαχειρίζονται τις μηχανές αναζήτησης. Αυτό όμως θα απαιτούσε εξιδικευμένες γνώσεις και πλήρη κατανόηση του κειμένου της πολιτικής μίας μηχανής αναζήτησης ή και ακόμα τον αποκλεισμό του χρήστη από κάποιες υπηρεσίες.

Η περίπτωση όμως αυτή φαντάζει αδύνατη επειδή ο μέσος χρήστης δεν έχει τις απαιτούμενες γνώσεις και πόσο μάλλον σε μία κοινωνία που συνεχώς αυξάνεται η ανάγκη για πληροφορίες δεν θα πρέπει να παρουσιάζετε σαν λύση η αποχή από οποιασδηποτε μορφή ηλεκτρονικής υπηρεσίας.

Έτσι τα κενά για την περιφρούριση της ιδιωτικότητας έρχεται να τα καλύψουν τα νομικά πλαίσια των χωρών. Πολλές φορές όμως από ότι γίνεται και αντιλιπτό στην εργασία η ταχύτητα με την οποία αναπτύσετε η τεχνολογία δημιουργεί ένα « κενό » . Για αυτό το λόγο μπορεί να θεωριθεί ότι τα νομοθετικά πλαίσια έχουν, στις περισσότερες των περιπτώσεων, τον ρόλο της περιφρούρησης της ιδιωτικότητας των χρηστών και την επιβολή κυρώσεων σε αυτούς που θα τα παραβούν .

Για την πρόληψη υπάρχουν τεχνολογίες, και έρευνες στον τομέα τομέα της ασφάλειας οι οποίες μπορούν να προσφέρουν μία ανώνυμη περιήγηση στον χρήστη, προστατεύοντας την ιδιωτικότητά του και τα οποία εξελίσονται συνεχώς όπως εξελίσονται και οι μηχανές αναζήτησης.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Βιβλιογραφία

---

[i] **http://comminfo.rutgers.edu/~ssaba/550/Week05/History.html**

[ii] **http://www.msit2005.mut.ac.th/msit_media/1_2549/ITEC5611/Materials/Optimizing%20for%20Crawlers.pdf**

[iii] **Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνιες Η νομική διάσταση Λίλιαν Μήτρου Τμήμα Μηχανικών & Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου**

[iv] **http://www.intgovforum.org/cms/Feb_igf_meeting/13_February_Consult_2007.txt**

[v] **http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html**

[vi] **Ruth Gavison, Privacy, 89 YALE L.J. 421 (1980); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Charles Fried, Privacy, 77 YALE L.J. 475 1968);**

[vii] **Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477 (2006**

[viii] **Ibid, id p.507.**

[ix] **Ibid, id**

[x] **Ibid, id note 17 and accompanying text.**

[xi] **http://ec.europa.eu/**

[xii] **http://ec.europa.eu/**

[xiii] **http://www.minpress.gr**

[xiv] **http://dide.fth.sch.gr/lows/n2472_97.html**

[xv] **ό.π, σ. 1467 σημ. 166.**

[xvi] **http://export.gov/safeharbor/**

[xvii] **http://export.gov/safeharbor/eu/eg_main_018475.asp**

[xviii] **DAVID BRIN, THE TRANSPARENT SOCIETY – WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).**

[xix] **http://www.ietf.org/proceedings/77/slides/plenaryt-5.pdf**

[xx] **http://www.research.att.com/ ~ Bala / newspapers/ pmob.pdf.**

[xxi] **Susan W. Brenner & Leo L. Clarke, Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data, 14 J.L. & POL'Y 211, 265 (2006).**

[xxii] **Dye, Jessica. "Consumer Privacy Advocates Seek Search Engine Solution".**

[xxiii] **IP Address, WIKIPEDIA, available at http://en.wikipedia.org/wiki/IP_address**

[xxiv] **CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS**

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

[xxv] **Ibid note 40.**

[xxvi] **Ryan Singel, Google Changes Cookie Policy but Privacy Effect is Small, WIRED BLOG NETWORK, July 16, 2007, available at http://blog.wired.com/27bstroke6/2007/07/google-changes- .html.**

[xxvii] **Article 29 Working Group Opinion 4/2007 on the concept of personal data, Jun. 20, 2007, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf,**

[xxviii] **Gemma Simpson, Google scores lowest in privacy rankings, ZDNET, Jun. 12, 2007, available at http://news.zdnet.co.uk/internet/0,1000000097,39287492,00.htm**

[xxix] **Privacy International, A Race to the Bottom - Privacy Ranking of Internet Service Companies, A Consultation report, Jun. 9, 2007, available at http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961**

[xxx] **ibid**

[xxxi] **Article 29 Working Party Press Release (07.08 2012), available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_21_06_07_en.pdf**

[xxxii] **In the Matter of Google and DoubleClick, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Apr. 20, 2007), available at http://www.epic.org/privacy/ftc/google/epic_complaint.pdf.**

[xxxiii] **Elinor Mills, Google buys ad firm DoubleClick for $3.1 billion, CNET NEWS.COM, Apr. 13, 2007, available at http://www.news.com/Google+buys+ad+firm+DoubleClick+for+3.1+billion/2100-1024_3-6176079.html?tag=st.rn.**

[xxxiv] **Joel Winston, Acting Associate Dir., Div. of Fin. Practices, FTC, Letter to Christine Varney, Esq., Jan. 22, 2001, available at http://www.ftc.gov/os/closings/staff/doubleclick.pdf**

[xxxv] **CNET news. Retrieved from http://news.cnet.com/2100-1030_3-6103098.html**

[xxxvi] **Pariser, Eli. "The Troubling Future of Internet Search"**

[xxxvii] **Blakeman, Karen. "What Search Engines Know About You"**

[xxxviii] **Cain Miller, C. (2012, January 25). A New Policy On Privacy From Google. The New York Times, p. B3**

[xxxix] **Steinhauser, G. (2012, February 3). Google's Privacy Policy Changes Prompt EU Probe. The Huffington Post. Retrieved from http://www.huffingtonpost.com/2012/02/03/google-privacy-policy_n_1253467.html**

[xl] **Miller, Claire (January 24, 2012). "Google To Update Privacy Policy to Cover Wider Data Use". New York Times.**

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

[xli] Reuters. (2012, February 1). Google defends change to privacy policies. Chicago Tribune. Retrieved from http://www.chicagotribune.com/business/breaking/chi-google-defends-change-to-privacy-policies-20120201,0,3821438.story

[xlii] James Canter, "E.U. Presses Google to Delay Privacy Policy Changes" 'The New York Times,' February 3, 2012

[xliii] Robert McMillan, "Google Relents, Will Hand Over European Wi-Fi Data" PC World

[xliv] "Google privacy policy is subject of backlash" 'The Washington Post.'

[xlv] EPIC – In re Facebook. (n.d.). EPIC – Electronic Privacy Information Center.12.08.2012

[xlvi] Jillian York "A Case for Psuedonyms" EFF.org, July 29, 2012

[xlvii] World, PC. "People Search Engines: Limit the Information They Can Collect". PC World. 11/08/12.

[xlviii] Brussels, 25.1.2012, COM(2012) 11 final σ.7 διαθέσιμο στο http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_el.pdf

[xlix] ό.π σ. 1

[l] ό.π σ. 2

[li] http://www.google.com/policies/privacy/archive/

[lii] Brussels, 25.1.2012, COM(2012) 11 final σ. 5

[liii] ό.π σ. 10

[liv] K. Sampigethaya, and R. Poovendran,A Survey on Mix Networks and Their Secure Applications, Proceedings of the IEEE,2006,94:12, 2142- 2181

[lv] M. Jakobsson, A. Juels, and R. Rivest, BMaking mix nets robust for electronic voting by randomized partial checking,[in Proc. USENIX' 02. New York: Springer-Verlag, 2002, pp. 339–353.

[lvi] L. Cottrell. (1994). Mixmaster and remailer Attacks. [Online]. Available: http://www.obscura.com/loki/remailer/remailer-essay.html

[lvii] L. Cottrell. (1994). Mixmaster and remailer Attacks. [Online]. Available: http://www.obscura.com/loki/remailer/remailer-essay.html

[lviii] M. Reiter, and A. Rubin, Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security, pp. 66-92, 1998.

[lix] S. Hongfei, w. Jianxin, C. Jianer, C. Songqiao, An analysis of forwarding mechanism in crowds, Communications, 2003. ICC '03. IEEE International Conference,2003,1, 261-265

[lx] M. Reiter, and A. Rubin, Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security, pp. 66-92, 1998

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

[lxi] S. Hongfei, w. Jianxin, C. Jianer, C. Songqiao, An analysis of forwarding mechanism in crowds, Communications, 2003. ICC '03. IEEE International Conference,2003,1, 261-265

[lxii] M. Reiter, and A. Rubin, Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security, pp. 66-92, 1998.

[lxiii] S. Hongfei, w. Jianxin, C. Jianer, C. Songqiao, An analysis of forwarding mechanism in crowds, Communications, 2003. ICC '03. IEEE International Conference,2003,1, 261-265

[lxiv] Landsiedel, O. , Pimenidis, A. ; Wehrle, K. ; Niedermayer, H. ; Carle, G. ,Dynamic Multipath Onion Routing in Anonymous Peer-To-Peer Overlay Networks,2007, Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, 64 - 69

[lxv] Landsiedel, O. , Pimenidis, A. ; Wehrle, K. ; Niedermayer, H. ; Carle, G. ,Dynamic Multipath Onion Routing in Anonymous Peer-To-Peer Overlay Networks,2007, Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, 64 - 69

[lxvi] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," IEEE Journal on Selected Areas in Communication, Special Issue on Copyright and Privacy Protection, 1998.

[lxvii] Landsiedel, O. , Pimenidis, A. ; Wehrle, K. ; Niedermayer, H. ; Carle, G. ,Dynamic Multipath Onion Routing in Anonymous Peer-To-Peer Overlay Networks,2007, Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, 64 - 69

[lxviii] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," IEEE Journal on Selected Areas in Communication, Special Issue on Copyright and Privacy Protection, 1998.

[lxix] R. Dingledine, N. Mathewson, P. Syverson,Tor: the second-generation onion router, SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium,2004,13:21

[lxx] PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval _Prateek Mittal, Femi Olumofin, Carmela Troncos,

[lxxi] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. In IEEE Annual Symposium on Foundations of Computer Science (FOCS 95), pages 41–50, 1995..

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ