Πανεπιστήμιο Πειραιώς – Τμήμα πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

"Πληροφορική"

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Κοινωνικά δίκτυα μέσω φορητών συσκευών: Η προστασία της θέσης**
Ονοματεπώνυμο φοιτητή	**Σπυρίδων Παράσχης**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΠΛ/06056**
Επιβλέπων	**Ε. Φούντας, Καθηγητής**

Ιούνιος 2012

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Ε. Φούντας	Μ. Βίρβου	Γ. Τσιχριντζής
Καθηγητής	Καθηγήτρια	Καθηγητής

Κατάλογος περιεχομένων

Εισαγωγή.....5

Πώς αποκαλύπτεται η θέση ενός χρήστη φορητής συσκευής.....8

Άμεσος εντοπισμός.....8

Έμμεσος εντοπισμός.....12

Κίνδυνοι που προκύπτουν.....14

Προστασία των δεδομένων θέσης του χρήστη - πώς τίθεται το πρόβλημα.....16

Προστασία στη φορητή συσκευή.....17

Λογισμικό σύνδεσης.....17

Γεωγραφική σήμανση.....18

Η προσέγγιση των λειτουργικών συστημάτων iOS και Android.....19

Χρήση και προστασία δεδομένων θέσης από το κοινωνικό δίκτυο.....24

Facebook.....24

Παρατηρήσεις.....26

Το Flickr.....31

Η περίπτωση του Google+.....33

Παρατηρήσεις, ελλείψεις και ευάλωτα χαρακτηριστικά.....36

Ιστορικά στοιχεία 41

Παράκαμψη των ρυθμίσεων ασφαλείας του Safari.....42

Καταγραφή δεδομένων από το Street View.....44

Καταγραφή κινήσεων από το iOS.....46

Το ισχύον νομικό πλαίσιο.....47

Ειδική προστασία.....48

Φορείς εκμετάλλευσης τηλεπικοινωνιών.....48

Φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας.....49

Γενική προστασία 50

Υποχρεώσεις που απορρέουν από τη νομοθεσία.....53

Ποιοι τρόποι προστασίας προτείνονται.....58
Αλγοριθμικές μέθοδοι.....58
Ανωνυμία.....59
Άλλες μέθοδοι.....68
Πολιτικές απορρήτου.....74
Περαιτέρω ζητήματα.....79
Βιβλιογραφία.....82

Εισαγωγή

Στα κοινωνικά δίκτυα, συγκρούεται η εγγενής απαίτηση να αποκαλύπτουν οι συμμετέχοντες χρήστες προσωπικά στοιχεία, ώστε να δημιουργηθούν οι απαραίτητες επαφές μεταξύ των μελών του δικτύου, με την ανάγκη να προστατευθούν τα δεδομένα προσωπικού χαρακτήρα. Τα τελευταία χρόνια, με τη διάδοση της πρόσβασης στα δίκτυα αυτά μέσω συσκευών με δυνατότητες τοπικού εντοπισμού, στα δεδομένα που χρειάζονται προστασία έχουν προστεθεί και τα δεδομένα θέσης του κάθε χρήστη.

Το παρόν κείμενο επιχειρεί να θέσει το πρόβλημα της προστασίας των δεδομένων θέσης και κίνησης χρηστών που μετέχουν μέσω φορητών συσκευών σε κοινωνικά δίκτυα, να εξετάσει την νομικό πλαίσιο που το διέπει και να παρουσιάσει τα βήματα που έχουν προταθεί προς την κατεύθυνση της επίλυσής του. Έμφαση έχει δοθεί σε φορητές συσκευής και δη σε smartphones με λειτουργικά συστήματα iOS και Android ενώ όσον αφορά τα κοινωνικά δίκτυα έχουν εξεταστεί περισσότερα το Facebook, το Flickr και το Google+.

Οι χρήστες του Διαδικτύου είναι ευαίσθητοι σε θέματα προστασίας της ιδιωτικότητάς τους. Η έρευνα των Hofflamn et al[1] από το 1999, έδειξε ότι "το 94% των χρηστών του Ιστού έχουν αποφύγει να παράσχουν προσωπικά δεδομένα σε ιστοτόπους που τους το ζήτησαν, ενώ το 40% αυτών που έχουν παράσχει δημογραφικά δεδομένα, έχουν μπει στη διαδικασία να επινοήσουν ψευδή στοιχεία".

1 Hoffman, Novak, and Peralta (1999)

Απ' την άλλη στο πλαίσιο της συμμετοχής σε κοινωνικά δίκτυα, οι χρήστες σκόπιμα αποκαλύπτουν προσωπικά τους στοιχεία. Ονοματεπώνυμο, προσωπικές φωτογραφίες, στοιχεία επικοινωνίας, σχολείο φοίτησης, τίτλος και χώρος εργασίας συγκαταλέγονται στα στοιχεία που πρόθυμα παρέχουν τα μέλη κοινωνικών δικτύων. Αυτή η πρακτική έχει ευαισθητοποιήσει ιδιαίτερα τους ερευνητές, κάποιοι εκ των οποίων υποστηρίζουν ότι έχουμε φτάσει στο "τέλος της ιδιωτικότητας"[2]. Η ανησυχία αυτή επιτείνεται από τον όγκο των προσωπικών στοιχείων και πληροφοριών που διακινούνται καθημερινά. Στο Facebook για παράδειγμα, τα περίπου 800 εκατομμύρια των μελών του κατά μέσο όρο "ανεβάζουν" καθημερινά περί τα 250 εκατομμύρια φωτογραφίες (στοιχεία Σεπτεμβρίου 2011)[3].

Η αποκάλυψη των προσωπικών δεδομένων στα κοινωνικά δίκτυα είναι κατά κανόνα ηθελημένη. Παρ' όλα αυτά, και σε αυτό το πλαίσιο τα προσωπικά δεδομένα χρήζουν προστασίας, αφού ο κύκλος των μερών που έχουν πρόσβαση στα δημοσιευμένα στοιχεία μπορεί να είναι πολύ ευρύτερος από αυτόν που επιθυμούσε ο χρήστης. Έτσι, έχουμε φαινόμενα όπως η χρήση των κοινωνικών δικτύων για τη διενέργεια ελέγχων των προς πρόσληψη εργαζομένων από εταιρίες[4] ή ακόμα και προς το σκοπό της εξιχνίασης εγκληματικών πράξεων[5]. Εκτός αυτού, παρατηρούνται και περιπτώσεις μη ηθελημένης αποκάλυψης στοιχείων. Στο Facebook για παράδειγμα, είναι

2 George Alisson (2006)

3 Facebook press info / Statistics, http://www.facebook.com/press/info.php?statistics

4 CareerBuilder: Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds. (2009)

5 Kate Maternowski (2006)

δυνατή η σήμανση (tagging) της παρουσίας ενός χρήστη, χωρίς προέγκρισή του προς αυτό, σε φωτογραφία τρίτου[6].

Η θέση ενός χρήστη είναι ένα από τα σημαντικότερα προσωπικά δεδομένα που χρήζουν προστασίας. Ταυτόχρονα συνιστά και μια πολύ ιδιαίτερη κατηγορία προσωπικών στοιχείων, γιατί η αποκάλυψή της, ακόμα και όταν γίνεται ηθελημένα, με την προέγκριση του χρήση, είναι μια συνεχής διαδικασία. Περισσότερα θα δούμε παρακάτω, αναφέροντας τους τρόπους εντοπισμού ενός χρήστη.

Η αποκάλυψη της θέσης είναι προϋπόθεση για την αξιοποίηση μιας σειράς υπηρεσιών, σε τομείς όπως το λογισμικό πλοήγησης / δρομολόγησης (π.χ. Google Maps navigation[7]), οι λιανικές πωλήσεις[8] και η εξεύρεση πληροφοριών με άμεσα τοπικό χαρακτήρα (για παράδειγμα η εφαρμογή "Vrisko", για συσκευές iPhone/iPad επιτρέπει την εξεύρεση των πλησιέστερων σταθμών βενζίνης ή φαρμακείων)[9].

Απ' την άλλη, η αποκάλυψη της θέσης, εντός και εκτός κοινωνικών δικτύων, συνιστά και πηγή σημαντικών κινδύνων. Για παράδειγμα, σύμφωνα με άρθρο της USA Today[10], παρατηρήθηκε το 2009 στο Michigan και στο Ohio σωρεία κλοπών συσκευών GPS από αυτοκίνητα παρκαρισμένα σε εμπορικά κέντρα. Χρησιμοποιώντας την καταγεγραμμένη στη συσκευή GPS διεύθυνση

6 Facebook photo tagging feature, http://www.facebook.com/help/tagging

7 http://maps.google.com

8 Andrew E. Fano (1998)

9 Vrisko, από τη Newsphone S.A., http://itunes.apple.com/gr/app/vrisko/id444977780?mt=8

10 Chris Woodyard (21-12-2009)

κατοικίας του ιδιοκτήτη, οι εγκληματίες κατευθύνθηκαν στα κατά εύλογη πιθανολόγησή τους άδεια σπίτια και τα διέρρηξαν. Χαρακτηριστική είναι και η περίπτωση ιστοσελίδων, όπως η PleaseRobMe.com και η icanstalku.com, που ψάχνει στο λογαριασμό ενός χρήστη Twitter για αναφορές της παρουσίας του σε συγκεκριμένους χώρους και βάσει αυτών απεικονίζει τη θέση του και σε κάποιες περιπτώσεις και τη διαδρομή του. Προφανώς, αν πρακτικές όπως το cyberstalking, δηλαδή η παρακολούθηση, ενόχληση ή και τρομοκράτηση ενός ατόμου μέσω του διαδικτύου είναι μια θλιβερή πραγματικότητα[11], η αποκάλυψη της θέσης κάποιου ανοίγει το δρόμο για να μετατραπούν οι ψηφιακές αυτές επιθέσεις σε επιθέσεις στον πραγματικό κόσμο.

Πώς αποκαλύπτεται η θέση ενός χρήστη φορητής συσκευής

Γενικά, η αποκάλυψη της θέσης μιας συσκευής μπορεί να είναι άμεση ή έμμεση. Η άμεση αποκάλυψη γίνεται με τον γεωγραφικό εντοπισμό της συσκευής, με την οποία ο χρήστης συνδέεται στο δίκτυο, ενώ η έμμεση γίνεται στο πλαίσιο αναγραφής άλλων πληροφοριών, που εμπεριέχουν στοιχεία γεωγραφικού εντοπισμού.

Άμεσος εντοπισμός

– Αν η συσκευή του χρήστη διαθέτει δέκτη GPS, η θέση του μπορεί να εξακριβωθεί με μεγάλη ακρίβεια (2 – 20 μέτρα). Το GPS πάντως δε δουλεύει σε εσωτερικούς χώρους (απαιτείται ανεμπόδιστη θέα προς τον

11 Huffaker (2006)

ουρανό, έστω και υπό γωνία, για τη σύνδεση με τουλάχιστον 4 δορυφόρους[12]) και σε αστικές περιοχές με ψηλά κτίρια γύρω-γύρω (urban canyons), επίσης ενδέχεται να μην μπορεί να λειτουργήσει. Ο εντοπισμός της θέσης γίνεται από τη συσκευή του χρήση και αποστέλλεται στο κοινωνικό δίκτυο.

– Αν η συσκευή του χρήστη είναι ένα κινητό τηλέφωνο, η θέση του μπορεί να εντοπιστεί από τον πάροχο κινητής τηλεφωνίας βάσει της κυψέλης του δικτύου στην οποία ο χρήστης συνδέεται (ή από το συνδυασμό των επικαλυπτόμενων κυψελών). Σε αστικές περιοχές, όπου τα δίκτυα κινητής τηλεφωνίας είναι πυκνότερα, η ακρίβεια εντοπισμού μπορεί να είναι κατ' ελάχιστο περί τα 50 μέτρα, ενώ σε περιοχές με αραιότερη κάλυψη, η ακρίβεια περιορίζεται σε ακτίνες αρκετών χιλιομέτρων. Στη μέθοδο αυτή, τη θέση του χρήστη μπορεί να γνωρίζει ο πάροχος κινητής τηλεφωνίας. Για να γίνει αυτή γνωστή στην οποιαδήποτε υπηρεσία απαιτεί τη γνώση της θέσης, μέχρι πρότινος ήταν απαραίτητη η συνεργασία του παρόχου[13]. Πλέον, όπως θα δούμε και παρακάτω, αυτό δεν ισχύει, χάρη σε προσπάθειες χαρτογράφησης και αποτύπωσης της θέσης των κεραιών κινητής τηλεφωνίας, που έχουν καταγραφεί σε βάσεις δεδομένων είτε ιδιωτικές (όπως η περίπτωση των Google Maps) είτε ελεύθερες (όπως το OpenCellId). Χάρη στα στοιχεία που περιέχουν και με αφετηρία ότι μια τηλεφωνική συσκευή γνωρίζει σε ποια κεραία συνδέεται, έχει καταστεί δυνατός ο αρκετά ακριβής εντοπισμός ενός κινητού τηλεφώνου μέσω του δικτύου κινητής

12 Weyn and Schrooyen (January 31, 2008)

13 Kaasinen (2003)

τηλεφωνίας ακόμα και χωρίς τη συμμετοχή του παρόχου. Χαρακτηριστική περίπτωση εντοπισμού με αυτή τη μέθοδο είναι η δικαστική υπόθεση της δολοφονίας Damilola Taylor, κατά την οποία οι βασικοί ύποπτοι απαλλάχθηκαν γιατί με βάση τα κινητά τους τηλέφωνα, αποκαλύφθηκε ότι ήταν 2 μίλια μακριά από το σημείο του φόνου, κατά την ώρα τέλεσής του.[14]

– Μια άλλη μέθοδος εντοπισμού[15] χρησιμοποιείται στην περίπτωση σύνδεσης μέσω ασύρματου δικτύου (WiFi). Παρ' ότι το Wifi δεν έχει σχεδιαστεί για τοπικό εντοπισμό, τα ραδιοκύματά του μπορούν να χρησιμοποιηθούν προς αυτό το σκοπό, χρησιμοποιώντας την τιμή της έντασης του ειλημμένου σήματος (Received Signal Strength – RSS), που παρέχεται από οποιαδήποτε συσκευή έχει δυνατότητα WiFi. Αυτή η τιμή μας δίνει την απόσταση της συσκευής από το σημείο πρόσβασης. Αν έχουμε ένα πυκνό δίκτυο ασύρματων σημείων πρόσβασης, με γνωστή τη θέση τους, η εγγύτητα του χρήστη σε αυτά μπορεί να χρησιμοποιηθεί για τον εντοπισμό του. Η ακρίβεια ποικίλει ανάλογα με την πυκνότητα του δικτύου ενώ η δυνατότητα άμεσου εντοπισμού παύει όταν ο χρήστης βρεθεί εκτός εμβέλειας του ασύρματου δικτύου.

Όπως διαγράφεται η εικόνα στις τεχνολογίες εντοπισμού, παρατηρούμε ότι κάθε τεχνολογία έχει σαφή πλεονεκτήματα και μειονεκτήματα. Το GPS προσφέρει ακρίβεια αλλά δε λειτουργεί καλά σε εσωτερικούς χώρους, ο εντοπισμός βάσει της κυψέλης κινητής έχει μεγάλο εύρος ακρίβειας και απαιτεί τη σύνδεση μέσω GSM, ενώ το WiFi περιορίζεται σε τοπικό επίπεδο. Έτσι,

14 Peter Stubley (2006)

15 Krumm and Horvitz (2004)

έχουν προταθεί και πολλές μέθοδοι συνδυασμού αυτών των τεχνολογιών, τόσο σε θεωρητικό επίπεδο (π.χ. Weyn and Schrooyen, January 31, 2008[16], Zirari, Canalda, and Spies, 2010[17]), όσο και σε πρακτικό επίπεδο (π.χ. η τεχνολογία gpsOne που σχεδίασε η QUALCOMM για δίκτυα CDMA[18] και τη τεχνολογία A-GPS που εφαρμόζεται κατά κόρον σήμερα[19]).

Ενδιαφέρουσα είναι και η προσέγγιση του λειτουργικού Android της Google στο ζήτημα του εντοπισμού μέσω των κυψελών του δικτύου κινητής τηλεφωνίας. Κάθε συσκευή που χρησιμοποιεί το Android, λειτουργεί στο δίκτυο κινητής τηλεφωνίας και και είναι εξοπλισμένη με GPS, αποστέλλει σε κάθε χρήση της εφαρμογής χαρτογράφησης Google Maps τις γεωγραφικές συντεταγμένες της τρέχουσας θέσης της και το μοναδικό αναγνωριστικό (Cell-Id) της κεραίας κινητής τηλεφωνίας στην οποία είναι συνδεδεμένη. Αναλύοντας αυτά τα δεδομένα, η Google έχει συνθέσει μια βάση δεδομένων με τις θέσεις των κεραιών κινητής τηλεφωνίας. Έτσι, όταν ζητείται η θέση μιας συσκευής χωρίς GPS, η Google μπορεί να παράσχει τη σχετική πληροφορία, χωρίς τη μεσολάβηση του παρόχου κινητής τηλεφωνίας, ενώ παλιότερα ο εντοπισμός αυτός γινόταν μόνο με τη μεσολάβηση και συνεργασία του παρόχου.[20] Παρεμφερείς προσπάθειες για τη δημιουργία βάσεων δεδομένων που συσχετίζουν Cell-id και γεωγραφικές συντεταγμένες έχουν γίνει και άλλες,

16 Weyn and Schrooyen (January 31, 2008)
17 Zirari, Canalda, and Spies (2010)
18 Soliman et al. (2000)
19 Jarvinen, DeSalas, and LaMance (2002)
20 Zhengrong and Jain (June 6, 2008)

όπως το Mobile Location των Ericcson Labs[21], το OpenCellId[22], το Cell Spotting[23] και το Skyhook.[24].

Αξίζει να σημειωθεί ότι η διερεύνηση της διεύθυνση IP μιας συσκευής που συνδέεται στο Διαδίκτυο συνιστά επίσης μια διαδεδομένη μέθοδο γεωγραφικού εντοπισμού μικρής σχετικά ακρίβειας με πλούσια σχετική έρευνα (π.χ. Guo et al., 2009), αλλά στην περίπτωση σύνδεσης μέσω GSM/3G, ο εντοπισμός, λόγω της συνεχούς εναλλαγής διεύθυνσης και εισόδου σε άλλους τομείς δικτύου, καθίσταται ιδιαίτερα ανακριβής ή ακόμα και λανθασμένος, όπως αποδεικνύει η έρευνα των Feldmann et al.[25]

Έμμεσος εντοπισμός

Ο έμμεσος εντοπισμός της θέσης ενός χρήστη γίνεται λιγότερο σε τεχνικό και περισσότερο σε ανθρωποκεντρικό επίπεδο. Ο χρήστης που φωτογραφίζει κατά τις διακοπές του ένα αξιοθέατο και "ανεβάζει" αμέσως στο Twitter τη φωτογραφία, προφανώς αποκαλύπτει τη θέση του. Ομοίως και αυτός που περιγράφει στο Facebook πόσο ωραία περνάει στις διακοπές του στο Παρίσι, λέει εν γνώσει του (ίσως όμως χωρίς να λαμβάνει υπ' όψη τις συνέπειες) πού βρίσκεται. Ακόμα και χωρίς καν τη ευθύνη και συμμετοχή του μπορεί κάποιος να δει τη θέση του να εκτίθεται σε ένα κοινωνικό δίκτυο, όταν επισημαίνεται η παρουσία του σε μια φωτογραφία (tagging) από έναν τρίτο,

21 https://labs.ericsson.com/apis/mobile-location/
22 http://opencellid.org/
23 http://www.cellspotting.com/webpages/cellspotting.html
24 http://www.skyhookwireless.com/
25 Feldmann et al. (2009)

συσχετιζόμενο με αυτόν ("φίλο" του), στο δίκτυο.

Μια πιο ενδιαφέρουσα και "κρυφή" περίπτωση είναι το geotagging φωτογραφιών, δηλαδή η συμπερίληψη σε μια φωτογραφία των συντεταγμένων της θέσης στην οποία έγινε η λήψη της. Η δυνατότητα geotagging παρέχεται από όλα σχεδόν τα εξελιγμένα κινητά τηλέφωνα τύπου smartphone, που είναι εξοπλισμένα με δέκτη GPS και φωτογραφική μηχανή, ενώ πλέον υπάρχουν ακόμη και φωτογραφικές μηχανές, με τέτοιες δυνατότητες, όπως η Canon PowerShot SX210 IS[26]. Ακόμα, η αποτύπωση των γεωγραφικών συντεταγμένων μπορεί να γίνει και με επεξεργασία των φωτογραφιών εκ των υστέρων, δυνατότητα που υποστηρίζεται σε υπηρεσίας κοινής διάθεσης φωτογραφιών, όπως το Picassa και το Flickr. Χαρακτηριστική και αρκετά προβεβλημένη περίπτωση μη ηθελημένης αποκάλυψης ζωτικής σημασίας πληροφοριών είναι η περίπτωση του Adam Savage, Αμερικανού παρουσιαστή της εκπομπής Mythbusters, που φωτογράφισε με το iPhone του το αυτοκίνητό του έξω από το σπίτι του και "ανέβασε" τη φωτογραφία στο Twitter, με το σχόλιο "Off to work now". Με αυτόν τον τρόπο αποκάλυψε το πού μένει, τι αυτοκίνητο έχει και ποια ώρα απουσιάζει από το σπίτι του.[27]

Οι Friedland και Sommer[28] εξερεύνησαν τη δυνατότητα εύρεσης της ακριβούς διεύθυνσης ανθρώπων βάσει φωτογραφιών και βίντεο που έχουν "ανεβάσει" στους ιστοτόπους των YouTube, Twitter, Craigslist και Flickr. Είανι

26 http://www.canon-europe.com/For_Home/Product_Finder/Cameras/Digital_Camera/PowerShot/PowerShot_SX210_IS/

27 Kate Murphy (11-8-2010)

28 Friedland and Sommer (2010)

Εικόνα 1: Φωτογραφία ενός ποδηλάτου προς πώληση και απεικόνιση της θέσης του από το Google Street View, βάσει του geotag της φωτογραφίας

χαρακτηριστικό ότι βάσει των δεδομένων γεωσήμανσης φωτογραφιών, μπόρεσαν να βρουν την ακριβή διεύθυνση χρηστών που είχαν αναρτήσει αγγελίες πώλησης ειδών στον κατάλογο του Craigslist και δεν είχαν συμπληρώσει τη διεύθυνσή τους, προφανώς μη επιθυμώντας την αποκάλυψή της. Για το σκοπό αυτό χρησιμοποίησαν τα γεωγραφικά μεταδεδομένα των φωτογραφιών που είχαν επισυνάψει στις αγγελίες τους και την υπηρεσία του Google Street View (εικόνα 1).

Κίνδυνοι που προκύπτουν

Οι φορητές συσκευές έχουν σχεδόν αποκλειστικά προσωπικό χαρακτήρα και επομένως κάθε συσκευή συνδέεται άμεσα με ένα συγκεκριμένο άτομο. Οι περισσότεροι άνθρωποι γνωρίζουν ότι η κινητή συσκευή τους περιέχει πολύ προσωπικές πληροφορίες, από μηνύματα ηλεκτρονικού ταχυδρομείου και προσωπικές φωτογραφίες έως ιστορικό περιήγησης και λίστες επαφών.

Αυτή η πραγματικότητα δίνει τη δυνατότητα στους παρόχους υπηρεσιών

κοινωνικής δικτύωσης με δυνατότητες εντοπισμού να καταρτίσουν πολύ λεπτομερή προφίλ για τους κατόχους μιας συσκευής. Η κατοικία ενός χρήστη προκύπτει από τη θέση της συσκευής το βράδυ. Η διεύθυνση εργασίας εξάγεται από το συνήθη πρωινό του προορισμό. Οι επαναλαμβανόμενες συνήθειες μετακίνησης και συσχετίσεις με φίλους επιτρέπουν την κατάρτιση ενός κοινωνικού γραφήματος[29], που περιγράφει τη σύνδεση των φίλων σε κοινωνικά δίκτυα και δίνει τη δυνατότητα εξαγωγής συμπερασμάτων σχετικά με συμπεριφορικά χαρακτηριστικά, βάσει δεδομένων για τους συγκεκριμένους φίλους. Αυτή η ανάλυση μπορεί επίσης να αποκαλύψει και ειδικές *κατηγορίες δεδομένων,* αν για παράδειγμα αποκαλύπτει επισκέψεις σε νοσοκομεία και χώρους θρησκευτικής λατρείας, συμμετοχή σε πολιτικές διαδηλώσεις.

Η τεχνολογία έξυπνων κινητών συσκευών παρέχει τη δυνατότητα διαρκούς παρακολούθησης των δεδομένων θέσης. Τα έξυπνα τηλέφωνα μπορούν να συλλέγουν διαρκώς σήματα από σταθμούς βάσης, δέκτες GPS και σημεία πρόσβασης wifi. Από τεχνικής άποψης, η παρακολούθηση μπορεί να γίνει μυστικά, εν αγνοία του κατόχου. Η παρακολούθηση μπορεί επίσης να διενεργείται με εν μέρει μυστικό τρόπο, σε περίπτωση που τα άτομα «ξεχνούν» ή αγνοούν το γεγονός ότι οι υπηρεσίες εντοπισμού θέσης είναι ενεργοποιημένες (στη θέση «on»), καθώς επίσης και όταν δεν ενημερώνονται για τυχόν αλλαγές βάσει των οποίων καθορίζεται η «ιδιωτική» ή «δημόσια» προσβασιμότητα.

Ακόμα και όταν τα άτομα καθιστούν εν γνώσει τους τα δεδομένα γεωγραφικής θέσης διαθέσιμα στο διαδίκτυο, μέσω των υπηρεσιών παροχής

29 http://developers.facebook.com/docs/reference/api/

πληροφοριών θέσης και γεωσήμανσης, η απεριόριστη πρόσβαση σε παγκόσμιο επίπεδο εγείρει νέους κινδύνους που κυμαίνονται από κλοπή δεδομένων και διάρρηξη έως σωματική επίθεση και παρενοχλητική παρακολούθηση.

Όπως και με άλλες νέες τεχνολογίες, ένας βασικός κίνδυνος από τη χρήση δεδομένων θέσης είναι η δυνατότητα υφέρπουσας διεύρυνσης λειτουργιών, δηλαδή το γεγονός ότι βάσει των νέων τύπων δεδομένων αναπτύσσονται νέοι σκοποί επεξεργασίας που δεν είχαν προβλεφθεί κατά την αρχική συλλογή δεδομένων.[30]

Όπως σημειώνουν οι Andrew J. Blumberg και Peter Eckersley σε άρθρο τους για τον Ίδρυμα Ηλεκτρονικού Μετώπου[31] (Electronic Frontier Foundation), αφ'ης στιγμής βγαίνουμε από το σπίτι μας, θυσιάζουμε μέρος της ιδιωτικότητάς μας. Αυτό που έχει σημασία στην παρακολούθηση της κίνησής μας μέσω φορητών συσκευών είναι ότι αυτός που ενδιαφέρεται να μας παρακολουθήσει δεν χρειάζεται να επενδύσει σε χρόνο και χρήμα. Η παρακολούθηση μπορεί να γίνει γρήγορα, ανέξοδα και εξ αποστάσεως από έναν κακόβουλο τρίτο, μια διαφημιστική εταιρία ή ακόμα και τις διωκτικές αρχές.

Προστασία των δεδομένων θέσης του χρήστη - πώς τίθεται το πρόβλημα

Βάσει όσων έχουν προαναφερθεί, το πρόβλημα της αποκάλυψης της

30 Γνωμοδότηση 13/2011 (16.5.2011) της Ευρωπαικής Ομάδας Εργασίας του άρθρου 29 για την προστασία των προσωπικών δεδομένων

31 https://www.eff.org/wp/locational-privacy

θέσης ενός χρήστη φορητής συσκευής στα κοινωνικά δίκτυα, τίθεται σε δύο βασικά επίπεδα: το πρώτο αφορά την ίδια τη φορητή συσκευή και το δεύτερο το κοινωνικό δίκτυο. Όσον αφορά τη συσκευή, εντοπίζεται στο λογισμικό σύνδεσης του χρήστη στο κοινωνικό δίκτυο (internet browser ή εξειδικευμένη εφαρμογή) και το πώς μέσω αυτού του λογισμικού προωθούνται και αποκαλύπτονται τα δεδομένα θέσης, καθώς και στη γεωγραφική σήμανση του υλικού (φωτογραφίες, βίντεο) και τον τρόπο που αυτή ελέγχεται από τον χρήστη. Όσον αφορά το κοινωνικό δίκτυο, μας ενδιαφέρει η χρήση και αξιοποίηση των δεδομένων θέσης από αυτό.

Προστασία στη φορητή συσκευή

Λογισμικό σύνδεσης

Σε μια φορητή συσκευή, η πρόσβαση στο κοινωνικό δίκτυο γίνεται είτε μέσω ενός προγράμματος περιήγησης στον Παγκόσμιο Ιστό (web browser), είτε, συνηθέστερα, με μια εξειδικευμένη εφαρμογή. Είναι προτιμότερη τόσο για τους τελικούς χρήστες, όσο και για τους παρόχους της υπηρεσίας η επιλογή της εξειδικευμένης εφαρμογής γιατί επιτρέπει την προσαρμογή του user interface στις ιδιαιτερότητες της φορητής συσκευής (μικρότερη οθόνη και υπολογιστική ισχύς) και την αξιοποίηση χαρακτηριστικών του υλικού (hardware) όπως η κάμερα και οι διάφοροι αισθητήρες. Βάσει αυτού, όλες οι γνωστές υπηρεσίες κοινωνικής δικτύωσης παρέχουν εφαρμογές για τα πιο διαδεδομένα λειτουργικά συστήματα φορητών συσκευών που εξετάσαμε, δηλ. το iOS και το

Android. Επιπλέον, κάποιες υπηρεσίες όπως το Facebook[32] και το Twitter[33], προσφέρουν μια προγραμματιστική πλατφόρμα που επιτρέπει την ανάπτυξη εφαρμογών τρίτων για την αξιοποίηση των υπηρεσιών του δικτύου και έτσι πέραν της επίσημης εφαρμογής για πρόσβαση στα εν λόγω δίκτυα, διατίθενται και πολλές άλλες "ανεπίσημες".

Σε κάθε περίπτωση, η σύνδεση με το κοινωνικό δίκτυο (και επομένως και η αποκάλυψη της τοποθεσίας) υπόκειται στο πλαίσιο που θέτει το λειτουργικό σύστημα της συσκευής για την εφαρμογή σύνδεσης, είτε πρόκειται για τον web browser είτε για μια ad hoc εφαρμογή.

Γεωγραφική σήμανση

Όπως έχει προαναφερθεί, η γεωγραφική σήμανση, φωτογραφιών κυρίως, (geotagging) συνιστά έναν διαδεδομένο και ενδεχομένως άγνωστο για πολλούς χρήστες τρόπο αποκάλυψης της τοποθεσίας τους. Η γεωγραφική σήμανση μπορεί να γίνει είτε από τη συσκευή που δημιουργεί το σημαινόμενο περιεχόμενο (φωτογραφία, video), είτε εκ των υστέρων, με εργαλεία που παρέχει το ίδιο το κοινωνικό δίκτυο. Η εκ των υστέρων σήμανση γίνεται επί τούτου από το χρήστη και γι' αυτό η προστασία της δεν μας ενδιαφέρει άμεσα στην παρούσα εργασία. Αντίθετα η σήμανση από την ίδια τη φορητή συσκευή, άνευ παρέμβασης του χρήστη, χρήζει περισσότερης μελέτης και προστασίας, κυρίως διότι πολλοί χρήστες αγνοούν τη σήμανση αυτή και την ακρίβειά της.

32 http://developers.facebook.com/

33 https://dev.twitter.com/

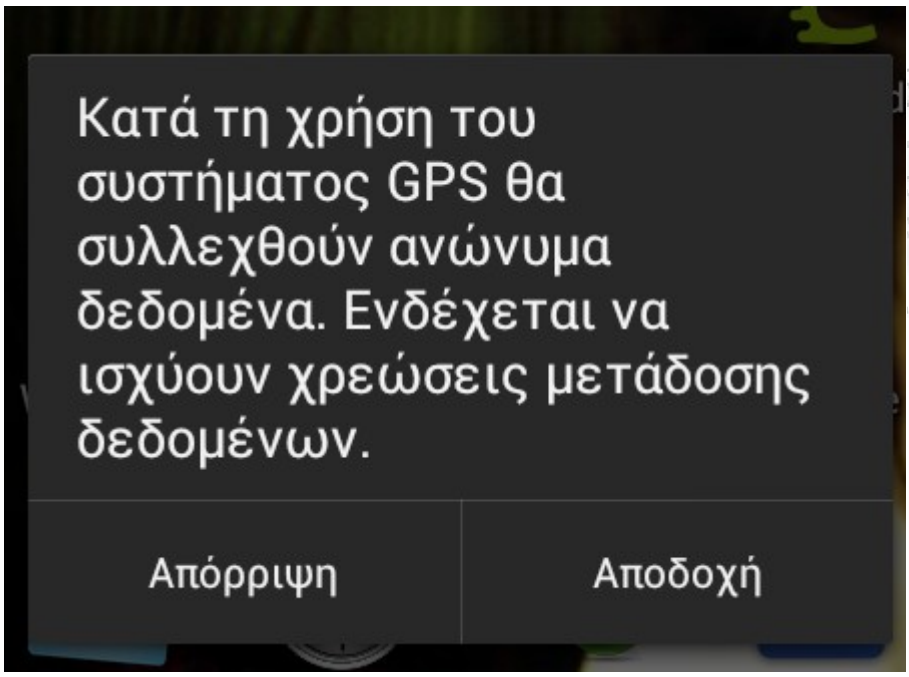
Η προσέγγιση των λειτουργικών συστημάτων iOS και Android

Στην παρούσα εργασία ελέγχθηκε ο τρόπος που τα πιο διαδεδομένα[34] λειτουργικά συστήματα φορητών συσκευών (Android και iOS) διαχειρίζονται το ζήτημα της προστασίας της θέσης του χρήστη.

Το λειτουργικό σύστημα Android[35] της Google επιτρέπει κατά την εγκατάσταση μιας εφαρμογής την παροχή έγκρισης για την πρόσβασή της στα δεδομένα θέσης της συσκευής. Αν δεν παρασχεθεί η έγκριση, η εφαρμογή δεν εγκαθίσταται. Τα δεδομένα θέσης διακρίνονται σε γνώση της ακριβούς τοποθεσίας (exact location) ή της τοποθεσίας κατά προσέγγιση (coarse location). Η λειτουργία geotagging είναι εξ ορισμού απενεργοποιημένη. Στην εικόνα 3 φαίνεται η λίστα των δικαιωμάτων (permissions) μιας εφαρμογής που απαιτεί τη γνώση της ακριβούς τοποθεσίας, όπως εμφανίζεται πριν από την εγκατάστασή της. Εκ των υστέρων δεν παρέχεται από το λειτουργικό η άμεση δυνατότητα στο χρήστη να μην επιτρέψει σε μια εφαρμογή την ενημέρωση για τη θέση της συσκευής. Φυσικά η δυνατότητα μπορεί να παρέχεται από την ίδια την εφαρμογή, ενώ ο χρήστης έχει πάντα τη δυνατότητα να απενεργοποιήσει όλα τα υποσυστήματα που χρησιμοποιεί η συσκευή για τον εντοπισμό της θέσης της, ήτοι το δέκτη GPS και τους πομποδέκτες WiFi και GSM. Φυσικά, σε μια τέτοια περίπτωση, η λειτουργικότητα της συσκευής μειώνεται σημαντικά.

34 http://blog.nielsen.com/nielsenwire/?p=29786

35 Εξετάστηκε η έκδοση 2.3 (Gingerbread)

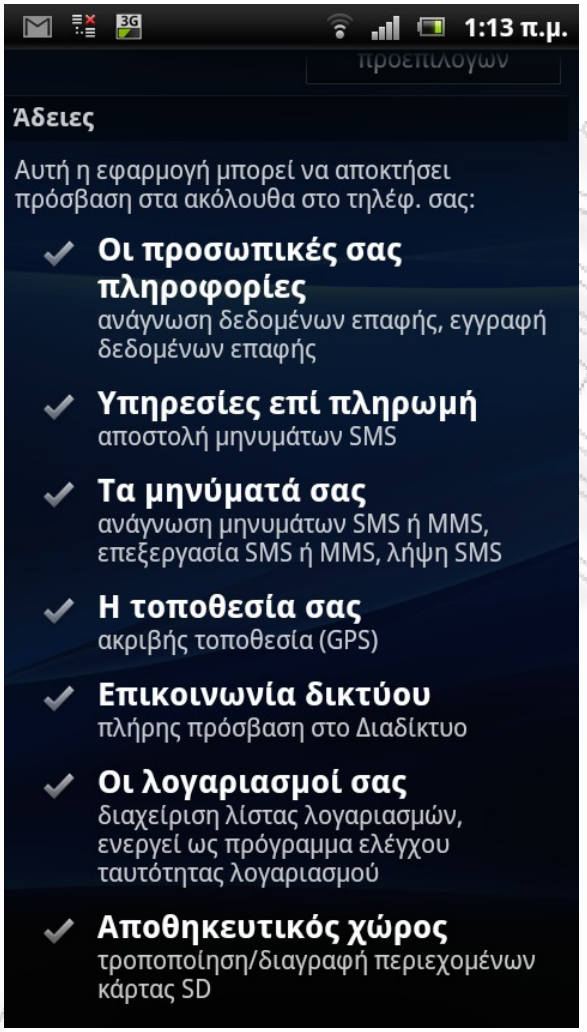


Εικόνα 2: Το μήνυμα του Android κατά την ενεργοποίηση του GPS

Ιδιαίτερη εντύπωση προκαλεί ότι κατά την ενεργοποίηση του GPS δέκτη της συσκευής, το Android ενημερώνει το χρήστη ότι κατά τη χρήση του GPS θα συλλεχθούν ανώνυμα δεδομένα θέσης και τον ρωτάει αν αποδέχεται αυτήν την πρακτική ή όχι. Η μη αποδοχή της συλλογής δεδομένων από το χρήστη απενεργοποιεί το δέκτη GPS. Είναι προφανές ότι αυτό το μήνυμα έχει τεθεί για νομικούς λόγους, ώστε να δίνεται αναγκαστικά η συναίνεση του χρήστη για τη συλλογή δεδομένων.

Το πρόγραμμα πλοήγησης του Android στο Διαδίκτυο υλοποιεί χαρακτηριστικά του Geolocation API του W3C[36], επιτρέποντας σε μια ιστοσελίδα να ζητήσει να μάθει τη θέση του χρήστη. Η έγκριση του χρήστη απαιτείται για

36 http://dev.w3.org/geo/api/spec-source.html



Εικόνα 3: Οθόνη παρουσίασης των δικαιωμάτων που απαιτεί μια εφαρμογή. Μέσα σε όλα διακρίνεται το δικαίωμα γνώσης της ακριβούς τοποθεσίας.

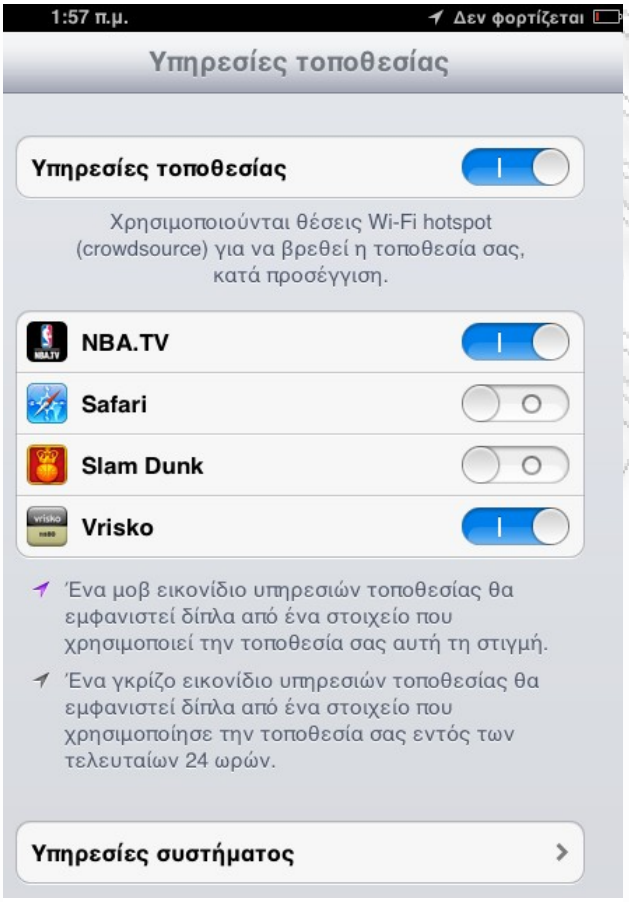
αυτό, χωρίς όμως να παρατίθενται πληροφορίες για τη σκοπούμενη χρήση των δεδομένων αυτών. Όταν δοθεί η έγκριση, δεν εμφανίζεται κάποια ένδειξη στην

οθόνη. Επίσης δεν παρέχεται κάποια δυνατότητα στο χρήστη να επεξεργαστεί τα στοιχεία των ιστοτόπων, οι οποίοι εχουν λάβει τη σχετική έγκριση. Επιτρέπεται η διαγραφή της πλήρους λίστας αυτών.

Τα λειτουργικό σύστημα iOS[37] της Apple, που χρησιμοποιείται στα iPhone, iPod touch και iPad, ζητάει από το χρήστη την έγκρισή του για να επιτρέψει την αποκάλυψη της θέσης του σε μία εφαρμογή. Η παροχή έγκρισης γίνεται ανά εφαρμογή, όπως φαίνεται στην εικόνα 4, και δεν αφορά τη λήψη φωτογραφιών, στις οποίες η γεωγραφική σήμανση (geotagging) είναι ενεργοποιημένη εξ ορισμού, αλλά ο χρήστης μπορεί να την απενεργοποιήσει. Επίσης η αιτούμενη έγκριση είναι απόλυτη – ο χρήστης δηλαδή μπορεί είτε να αποκαλύψει την ακριβή θέση του, είτε όχι, δεν μπορεί όμως να επιτρέψει σε μια εφαρμογή να γνωρίζει κατά προσέγγιση (σε επίπεδο νομού, ας πούμε), τη θέση του.

Ο browser του iOS (Safari) υποστηρίζει το Geolocation API. Η έγκριση του χρήστη απαιτείται για να εκπεμφθεί η θέση του σε εναν ιστότοπο. Όταν δοθεί η έγκριση και αποστέλλεται η θέση, εμφανίζεται μια οπτική ένδειξη, η οποία όμως δεν είναι εύκολα προσβάσιμη, αφού βρίσκεται στις ρυθμίσεις συστήματος. Όπως και στο Android, δεν παρέχεται κάποια δυνατότητα στο χρήστη να επεξεργαστεί τα στοιχεία των ιστοτόπων, οι οποίοι εχουν λάβει τη σχετική έγκριση. Σε κάθε επίσκεψη σε μια ιστοσελίδα που ζητάει πρόσβαση στη θέση του χρήστη, απαιτείται η ad hoc έγκριση.

37 Εξετάστηκε η έκδοση 5



Εικόνα 4: Οι επιλογές ενεργοποίησης ή μη των υπηρεσιών τοποθεσίας ανά εφαρμογή σε μια συσκευή iOS χωρίς GPS ή GSM (iPad 1ης γενιάς).

Αξίζει να σημειωθεί ότι οι παραπάνω παρατηρήσεις αφορούν συσκευές iOS και Android, στις οποίες ο χρήστης δεν έχει αποπειραθεί να παρακάμψει τους περιορισμούς που επιβάλλει το λειτουργικό σύστημα, ώστε να μπορεί να εκτελεί και εφαρμογές που βάσει των περιορισμών αυτών δεν θα επιτρεπόταν η εκτέλεσή τους. Στην περίπτωση του iOS η άρση των περιορισμών αυτών

καλείται "Jailbreak", ενώ στην περίπτωση του Android "rooting". Κάνοντας Jailbreak ή Rooting, ο χρήστης μπορεί να εκτελέσει εφαρμογές που υπερπηδούν περιορισμούς του Λ/Σ. Αυτό ενδέχεται να συνιστά και διακύβευση της προστασίας της θέσης του.

Χρήση και προστασία δεδομένων θέσης από το κοινωνικό δίκτυο

Όσον αφορά τα κοινωνικά δίκτυα, θα εξεταστεί ο τρόπος διαχείρισης των στοιχείων τοποθεσίας από το Facebook και το Google+ και της γεωγραφικής σήμανσης φωτογραφιών από το Flickr.

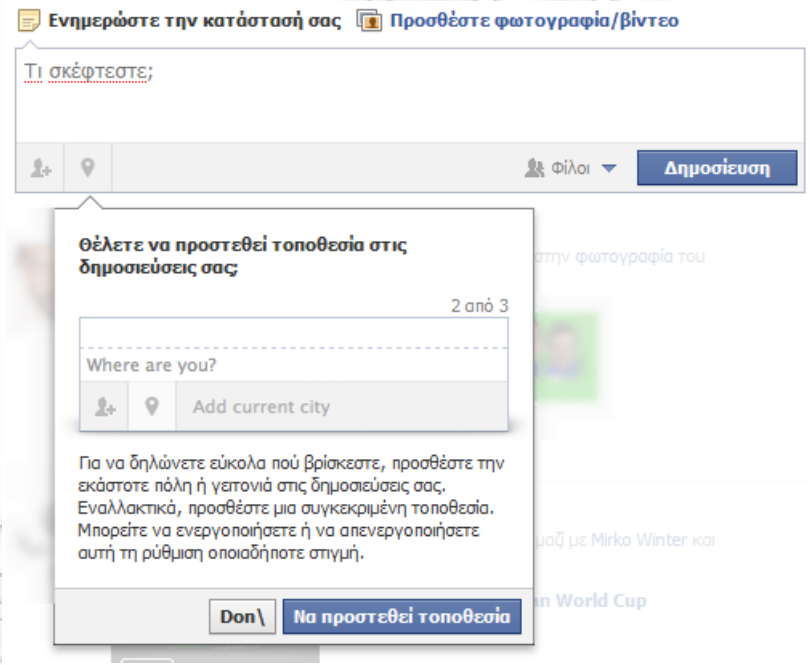
Facebook

Το Facebook επιτρέπει σε κάθε δημοσίευση την κοινοποίηση της τοποθεσίας του χρήστη[38], όπως φαίνεται στην εικόνα 5. Ο χρήστης μπορεί είτε να αποδεχτεί την περιοχή που του προτείνεται από το λογισμικό σύνδεσης, που είναι σε επίπεδο πόλης, είτε να αναγράψει μια ακριβέστερη τοποθεσία. Αν συνδέεται με φορητή συσκευή με δυνατότητες εντοπισμού, τότε η ακριβέστερη τοποθεσία μπορεί να προταθεί από τη συσκευή. Αν ο χρήστης δεν επιθυμεί να κοινοποιήσει τη θέση του, μπορεί να απενεργοποιήσει το εν λόγω χαρακτηριστικό. Αξίζει να σημειωθεί ότι ειδικά κατά τη σύνδεση με την εφαρμογή του Facebook για Android δεν φαίνεται ότι κοινοποιείται η τοποθεσία

38 http://www.facebook.com/help/location/about

του χρήστη κατά τη δημοσίευση – για να δει ο χρήστης ότι αυτό συμβαίνει πρέπει να μεταβεί σε μια άλλη φόρμα της εφαρμογής.

Πέραν της κοινοποίησης της θέσης του, ο χρήστης μπορεί κατά τη δημοσίευση να σημειώσει με ποιους "φίλους" του – μέλη του Facebook – βρίσκεται στην κοινοποιημένη θέση. Επιπλέον, μπορεί να καθορίσει τον κύκλο των αποδεκτών της δημοσίευσής του – και άρα τον κύκλο αυτών που θα μάθουν και τη θέση του, επιλέγοντας μεταξύ των φίλων του και όλων των χρηστών του Facebook.



Εικόνα 5: Δημιουργία νέας δημοσίευσης στο Facebook, με δυνατότητα κοινοποίησης της τοποθεσίας

Επιπλέον το Facebook υλοποιεί μια λειτουργία που καλεί "Τοποθεσίες" (Places). Στο πλαίσιο της λειτουργίας αυτής, "τοποθεσία" είναι μια γεωγραφικώς προσδιορισμένη περιοχή, για την οποία έχει δημιουργηθεί μια

σελίδα στο Facebook. Οι χρήστης μπορούν να κοινοποιήσουν ότι βρίσκονται σε μια τοποθεσία - η παρουσία τους αναγγέλλεται στη σελίδα του προφίλ τους και στη σελίδα της τοποθεσίας. Μέσω μιας φορητής συσκευής, ο χρήστης μπορεί να μάθει ποιες τοποθεσίες βρίσκονται κοντά του. Όπως και με μια απλή δημοσίευση, υπάρχει η δυνατότητα επιλογής των αποδεκτών μεταξύ όλων των χρηστών του Facebook ή μόνο των "φίλων" του χρήστη.

Κατά τη μεταφορά δεδομένων πολυμέσων στο Facebook τα στοιχεία γεωγραφικής σήμανσης που ενδεχομένως περιέχουν οι φωτογραφίες διαγράφονται. Δεν είναι σαφές αν αυτό γίνεται παρεπιπτόντως, λόγω της επεξεργασίας της εικόνας για μείωση του μεγέθους της και άρα της επιβάρυνσης των servers του Facebook, ή επί τούτου, ως μέτρο προστασίας της ιδιωτικότητας του χρήστη. Πάντως εκ των υστέρων ο χρήστης μπορεί να προσθέσει στοιχεία γεωγραφικής σήμανσης στις φωτογραφίες και στα βίντεό του. Τα στοιχεία αυτά δεν εγγράφονται στα αρχεία αλλά προφανώς διατηρούνται σε κάποια βάση δεδομένων στο server και επομένως αν ένας χρήστης "κατεβάσει" στον υπολογιστή του τα αρχεία αυτά, δεν μπορεί να εξάγει συμπεράσματα για τη θέση του χρήστη που τα δημοσίευσε.

Παρατηρήσεις

Θα πρέπει να σημειωθεί ότι το Facebook πολύ συχνά προβαίνει σε αναβάθμιση των υπηρεσιών του και σε αλλαγές των ρυθμίσεων ιδιωτικότητας, με αποτέλεσμα οποιαδήποτε παρουσίαση των πρακτικών του να διατρέχει τον κίνδυνο να κατασταθεί πολύ σύντομα παρωχημένη. Παρ' όλα αυτά,

παρατηρούμε μια συνεχή τάση οι προκαθορισμένες ρυθμίσεις για τα προσωπικά δεδομένα των χρηστών να τίθενται έτσι, ώστε να αποκαλύπτονται αυτά σε μεγάλο αριθμό αποδεκτών, πολλές φορές και εν αγνοία των χρηστών, αν δεν επιδιώξουν επι τούτου να αλλάξουν αυτές τις ρυθμίσεις. Επί παραδείγματι, στο κείμενο για την πολιτική απορρήτου του Facebook το 2005[39], διαβάζουμε ότι:

> *Οι προσωπικές πληροφορίες που εισάγετε στο Facebook δεν θα γίνονται γνωστές σε κανένα χρήστη του Διαδικτύου, αν αυτός δεν συμπεριλαμβάνεται στις ομάδες, που έχετε ορίσει στις ρυθμίσεις απορρήτου σας.*

Στο αντίστοιχο κείμενο για το 2009[40], διαβάζουμε ότι:

> *Το Facebook είναι σχεδιασμένο για να σας επιτρέπει εύκολα να μοιράζεται προσωπικές πληροφορίες με αυτούς που επιθυμείτε. Εσείς επιλέγεται πόσες πληροφορίες προτίθεστε να μοιραστείτε στο Facebook και ελέγχεται πώς θα γίνεται αυτό στις ρυθμίσεις απορρήτου σας. Θα πρέπει να ελέγξετε τις προκαθορισμένες ρυθμίσεις και να τις αλλάξετε κατά τις προτιμήσεις σας. Θα πρέπει επίσης να λαμβάνετε υπ' όψη σας αυτές τις ρυθμίσεις όταν εισάγετε δεδομένα στο Facebook. [….] Σε κατηγορίες πληροφοριών που είναι ρυθμισμένες "για όλους" μπορούν να έχουν πρόσβαση όλοι οι χρήστες του Διαδικτύου, ακόμα και αν δεν βρίσκονται στο Facebook, να καταγράφονται από μηχανές αναζήτησης τρίτων, να συνδέονται με εσάς και εκτός Facebook (όταν για παράδειγμα επισκέπτεστε άλλες ιστοσελίδες) και μπορούν να γίνονται αντικείμενο*

39 http://web.archive.org/web/20050809235134/www.facebook.com/policy.php
40 http://www.tosback.org/version.php?vid=961

επεξεργασίας από εμάς και τρίτους χωρίς περιορισμούς απορρήτου. ***Η προκαθορισμένη τιμή για κάποιες κατηγορίες πληροφοριών είναι "για όλους"****. Μπορείτε να ελέγξετε και να αλλάξετε αυτές τις τιμές στις ρυθμίσεις απορρήτου σας.*

Παρατηρούμε την τεράστια απόκλιση μεταξύ αυτών των δύο προσεγγίσεων. Ο ανεξάρτητος ερευνητής Matt McKeon[41] έχει καταγράψει τις διαφοροποιήσεις αυτές στην αποκάλυψη των προτιμήσεων (likes), των προσωπικών δεδομένων (όνομα, φωτογραφία προφίλ, γένος, ημερομηνία γέννησης, στοιχεία επικοινωνίας), των εκτεταμένων στοιχείων προφιλ (μέλη οικογένειας, τόπος γέννησης, σχολείο φοίτησης κλπ), των "φίλων", των ομάδων στις οποίες συμμετέχει ο χρήστης, των μηνυμάτων "τοίχου" και των φωτογραφιών και έχει συντάξει μια σειρά διαγραμμάτων που δείχνουν την σαφή τάση για την αλλαγή των προκαθορισμένων τιμών επί το αποκαλυπτικότερο με το πέρασμα του χρόνου (εικόνα 6).

Άμεση συνέπεια αυτού είναι ότι πολλές φορές οι χρήστες καταλήγουν εν αγνοία τους να αποκαλύπτουν πολύ περισσότερες προσωπικές πληροφορίες, απ' ότι θα επιθυμούσαν. Το 2011 για παράδειγμα, το Facebook ζήτησε από τα μέλη του να εισάγουν, προαιρετικά, τον αριθμό τηλεφώνου τους, ως ένα πρόσθετο μέτρο ασφάλειας, σε σε περίπτωση που έχαναν για κάποιο λόγο την πρόσβαση στη διεύθυνση e-mail, μέσω της οποίας ενεγράφησαν στο Facebook. Στη φόρμα εισαγωγής του αριθμού τηλεφώνου, υπήρχε ένα πεδίο που ενεργοποιούσε την εμφάνιση του εισηγμένου αριθμού σε όλους τους φίλους

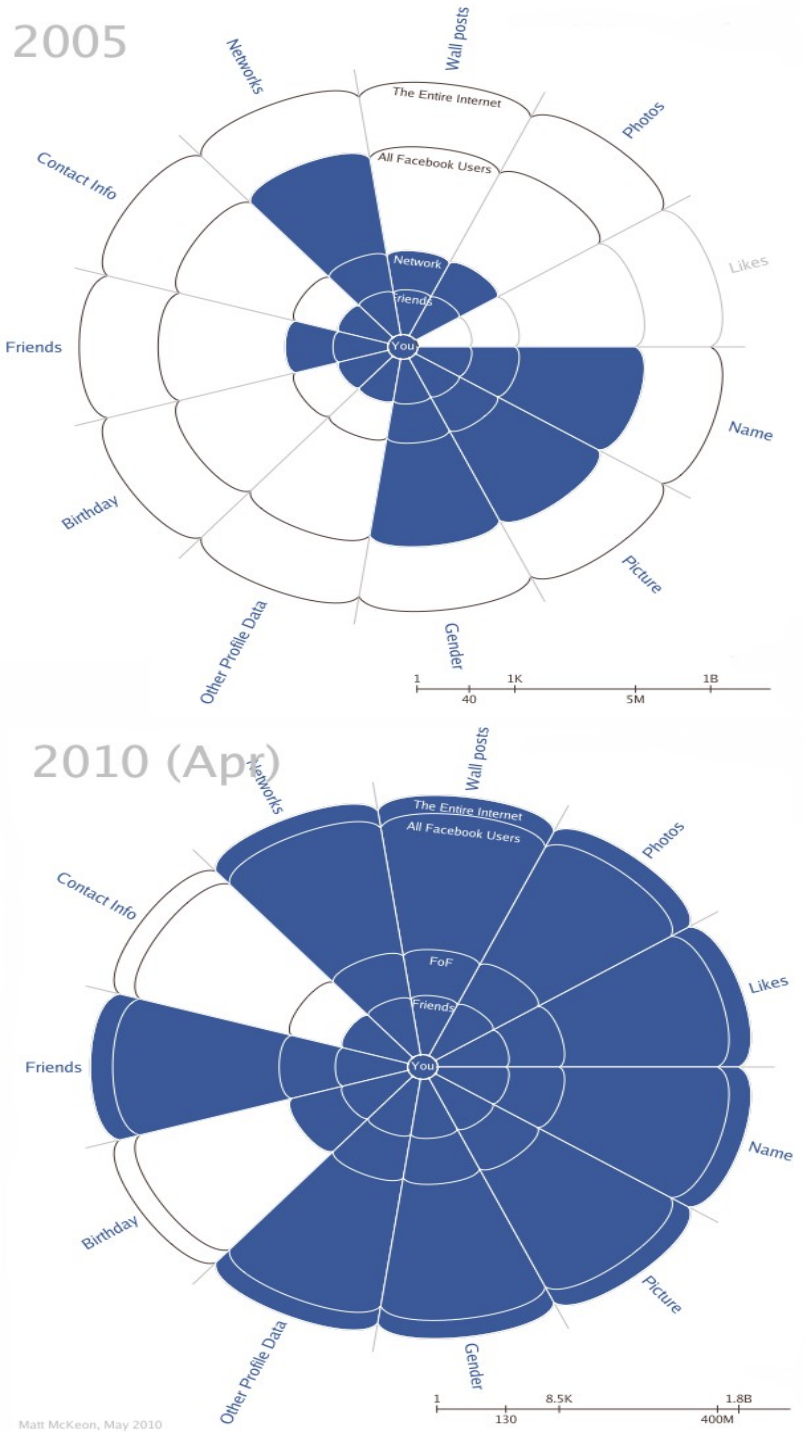
41 http://mattmckeon.com/facebook-privacy/

του χρήστη και ήταν εξ ορισμού επιλεγμένο. Αυτό είχε ως συνέπεια πολλοί χρήστες, λόγω απροσεξίας, να καταστήσουν γνωστό τον αριθμό του τηλεφώνου τους σε ένα μεγάλο, πέραν της επιθυμίας τους, κύκλο αποδεκτών.[42]

Ίσως η σαφέστερη και λακωνικότερη αποτύπωση της προσέγγισης του Facebook στην ιδιωτικότητα έρχεται από το συνιδρυτή της υπηρεσίας Mark Zugkerberg, που δήλωσε τον Ιανουάριο του 2010 ότι "η ιδιωτικότητα δεν είναι πλέον κοινωνική τάση".[43]

42 http://nakedsecurity.sophos.com/2011/08/11/has-facebook-got-your-mobile-number-now-your-friends-do-too/

43 http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy



Εικόνα 6: Γραφική αποτύπωση των προκαθορισμένων ρυθμίσεων του Facebook αναφορικά με το εύρος αποκάλυψης προσωπικών στοιχείων. Συγκρίνονται οι ρυθμίσεις των ετών 2005 και 2010.

Το Flickr

Το Flickr είναι ένα κοινωνικό δίκτυο με βασικό στόχο την παρουσίαση, σχολιασμό και αξιολόγηση φωτογραφιών. Είναι ιδιαίτερα δημοφιλές – τον Φεβρουάριο του 2012, σύμφωνα με τα στοιχεία του Alexa[44], ήταν ο 47ος πιο δημοφιλής ιστότοπος στο Διαδίκτυο.

Με δεδομένο ότι οι φωτογραφίες είναι στο επίκεντρο της λειτουργίας του Flickr, κατά τη μεταφορά τους σε αυτό δεν υφίστανται συμπίεση ή άλλη επεξεργασία που θα προκαλούσε αφαίρεση των μεταδεδομένων τους, όπως συμβαίνει στο Facebook. Αντ' αυτού, το Flickr επιτρέπει στο χρήστη να επιλέξει αν θα διατηρηθούν γενικά τα EXIF μεταδεδομένα της εικόνας (με προκαθορισμένη επιλογή το 'ΝΑΙ') και ειδικότερα αν θα διατηρηθούν μόνο τα μεταδεδομένα τοπικού εντοπισμού (με προκαθορισμένη επιλογή το 'ΟΧΙ').

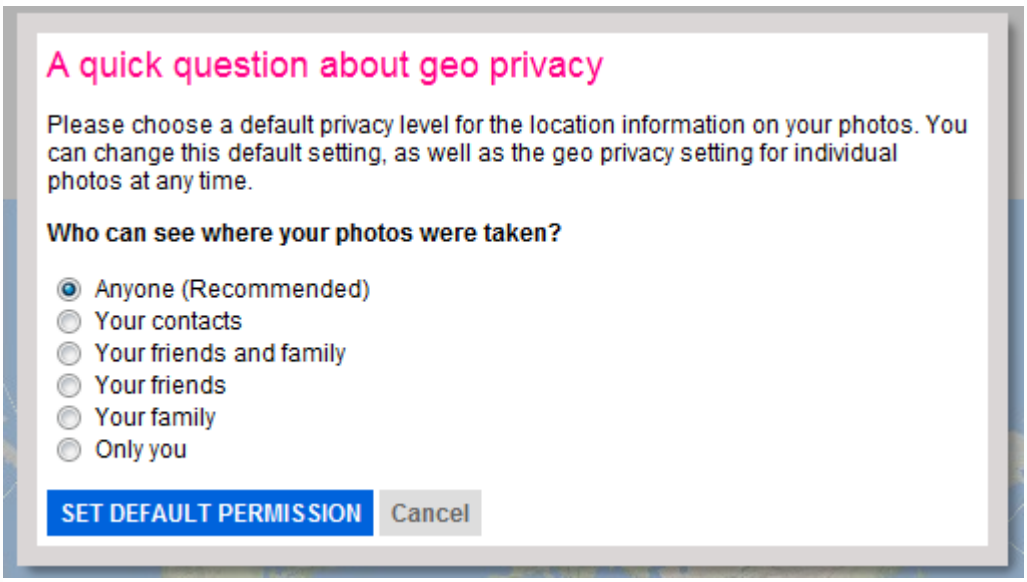
Επιπλέον, το Flickr υλοποιεί δύο χαρακτηριστικά που επιτρέπουν στο χρήστη να διαχειριστεί το ζήτημα προστασίας της θέσης του. Το πρώτο από αυτά επιτρέπει στον χρήστη να ορίσει ποιοι θα έχουν πρόσβαση στα μεταδεδομένα θέσης μιας φωτογραφίας, όπως φαίνεται στην εικόνα 7, επιλέγοντας μεταξύ των πάντων (ακόμη και επισκεπτών των φωτογραφιών του μη εγγεγραμμένων στο Flickr), των μελών του Flickr, των ορισμένων ως φίλων και μελών της οικογένειάς του (σωρευτικά ή διαζευκτικά), ή μόνο του εαυτού του. Η ρύθμιση μπορεί να αλλάξει ανά φωτογραφία.

Επιπλέον, το Flickr υλοποιεί ένα χαρακτηριστικό προστασίας των δεδομένων θέσης του χρήστη που το καλεί "Geofences"[45]. Βάσει αυτού, ο

44 http://www.alexa.com/siteinfo/flickr.com#

45 http://www.flickr.com/help/map/

χρήστης μπορεί να ορίσει στο χάρτη ένα χώρο εντός του οποίου τα στοιχεία γεωγραφικού εντοπισμού θα απενεργοποιούνται για τον κύκλο των προσώπων που επιθυμεί ο χρήστης. Έτσι, μπορεί κάποιος να ορίσει έναν τέτοιο "φράχτη" γύρω από το σπίτι του, ώστε να προστατεύσει την αποκάλυψη της διεύθυνσής του σε αγνώστους.



Εικόνα 7: Η φόρμα επιλογής του κύκλου που θα έχει πρόσβαση στις τοπικές πληροφορίες των φωτογραφιών ενός χρήστη

Αξίζει να σημειωθεί ότι αν η πρωτογενής φωτογραφία περιείχε μεταδεδομένα εντοπισμού στον τομέα EXIF του αρχείου της (δηλαδή δεν προστέθηκαν εκ των υστέρων γεωγραφικές ετικέττες), τότε όποιος τη βλέπει μπορεί να μεταφόρτωσει το πρωτότυπο αρχείο και να διαβάσει τα δεδομένα αυτά. Αυτό είναι μια συνέπεια της φύσης του Flickr ως φωτογραφικού

ενδιαφέροντος ιστοτόπου, που επιδιώκει να μην επεξεργάζεται τα πρωτότυπα αρχεία των φωτογραφικών, όπως αποστέλλονται από τα μέλη του. Στην περίπτωση αυτή, ο μόνος τρόπος προστασίας της θέσης, είναι, είτε να αποκλειστούν από την εμφάνιση της πρωτότυπης φωτογραφίας τα μέλη, που δεν πρέπει να μάθουν τη θέση αυτής, είτε η ενεργοποίηση της επιλογής για τη μη εισαγωγή των EXIF μεταδεδομένων τοπικού εντοπισμού.[46]

Η περίπτωση του Google+

Το Google+ είναι μια σχετικώς νέα προσπάθεια της Google για τη δημιουργία μιας υπηρεσίας κοινωνικής δικτύωσης ανταγωνιστικής του Facebook (*όλες οι παρατηρήσεις για τη λειτουργία του Google+ βασίζονται στη λειτουργία του μέχρι και τις 27 Φεβρουαρίου 2012*).

Στην καρδιά του Google+ βρίσκεται το χαρακτηριστικό "Circles" (Κύκλοι). Πρόκειται για την ένταξη των συνδεδεμένων με τον εκάστοτε χρήστη μελών σε κατηγορίες (καλούμενες "Κύκλοι"), για τις οποίες μπορεί να καθοριστεί διαφορετικό επίπεδο αποκάλυψης στοιχείων. Όπως αναγράφεται στην σχετική σελίδα[47] του Google+, "Οι κύκλοι διευκολύνουν τη οργάνωση, καθώς μπορείτε να τοποθετήσετε τους φίλους σας σε έναν κύκλο, τους γονείς σας σε κάποιον άλλο και το αφεντικό σας σε έναν κύκλο μόνο του· όπως συμβαίνει και στην πραγματική ζωή". Τα μέλη των κύκλων καθορίζονται από το

46 Όπως αναγράφεται στο Flickr (http://www.flickr.com/account/geo/privacy/?from=privacy): Please note: If you upload a photo with geo data, that info will be embedded in the EXIF data of the original file. If you don't want people to have access to this information, you should restrict who can download your originals.

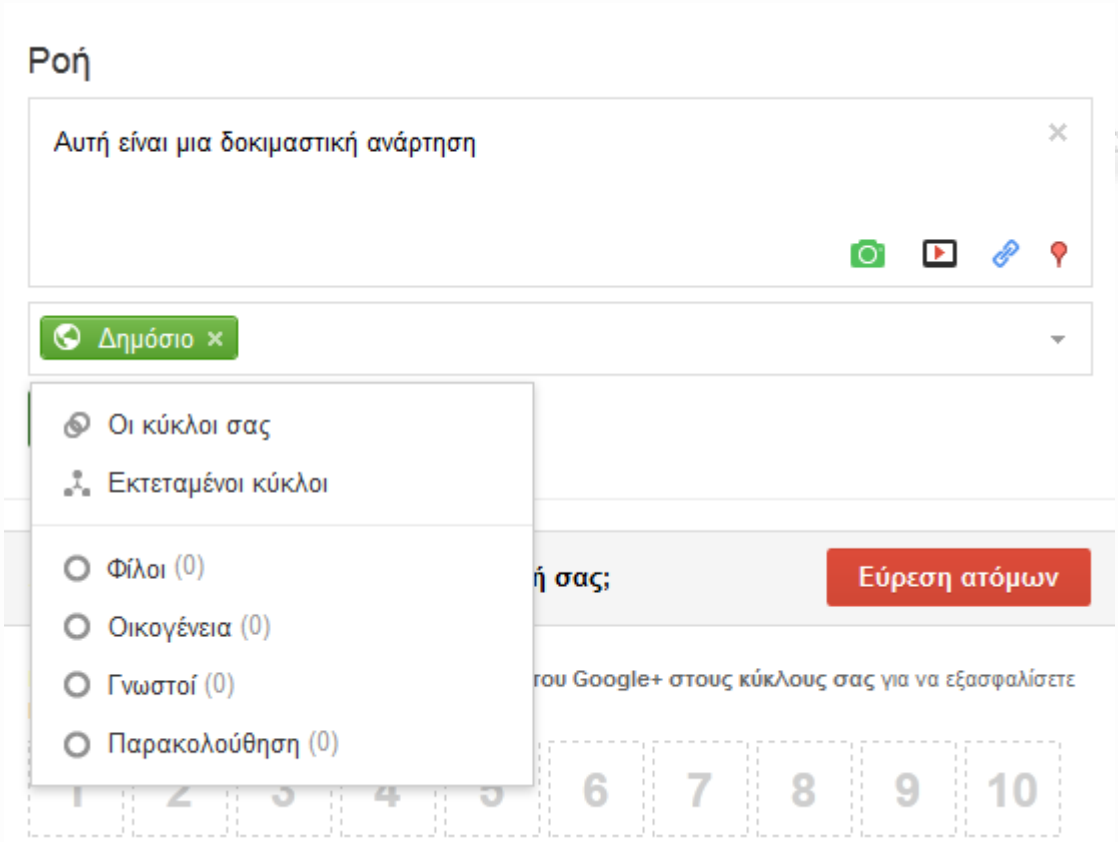
47 https://www.google.com/intl/el/+/learnmore/index.html#circles

χρήστη και ούτε αποκαλύπτεται σε τρίτους ποιους και πόσους "Κύκλους" έχει δημιουργήσει ένας χρήστης, ούτε σε κάποιον ενταγμένο σε έναν "Κύκλο" ποιοι άλλοι συμπεριλαμβάνονται σε αυτόν. Αυτό αποτρέπει την εξόρυξη δεδομένων για το χρήστη με τη χρήση τεχνικών όπως το Friend Classification που περιγράφουν οι Thomas et al.[48]

Η ανάρτηση της θέσης του χρήστη εντάσσεται και αυτή στην ίδια λογική κατηγοριοποίησης – ο χρήστης μπορεί σε κάθε ανάρτηση να προσθέσει την τρέχουσα θέση του και να καθορίσει σε ποιους "Κύκλους" θα εμφανιστεί η ανάρτηση μαζί με τη δήλωση της θέσης του.

Όσον αφορά τα μεταδεδομένα φωτογραφιών, που αναρτά ο χρήστης, στο Google Plus, όλα τα μεταδεδομένα διατηρούνται. Ο χρήστης όμως μπορεί να επιλέξει αν τα γεωγραφικά μεταδεδομένα θα εμφανίζονται ή όχι, αλλά αξίζει να σημειωθεί ότι η επιλογή αυτή είναι καθολική και όχι βάσει των κύκλων. Επιπλέον, ο χρήστης μπορεί να καθορίσει αν θα επιτρέπει τη μεταφόρτωση του πρωτότυπου αρχείου μιας φωτογραφίας ή όχι. Η επιλογή αυτή είναι σημαντική, γιατί το πρωτότυπο αρχείο περιλαμβάνει και τα γεωγραφικά μεταδεδομένα. Επομένως, απενεργοποιώντας την εμφάνιση των γεωγραφικών πληροφοριών και τη μεταφόρτωση του πρωτότυπου αρχείου, ο χρήστης μπορεί να αποτρέψει την αποκάλυψη της τοποθεσίας λήψης μιας φωτογραφίας.

48 Thomas, Grie, and Nicol ()



Εικόνα 8: Το interface εισαγωγής νέας ανάρτησης στο Google Plus (μέσω browser υπλογιστή). Φαίνονται τα εικονίδια προσθήκης της θέσης του χρήστη και ο καθορισμός των κύκλων αποδεκτών. της ανάρτησης.

Κατά τη χρήση σε φορητές συσκευές, όπως σαφώς αναγράφεται στην πολιτική απορρήτου[49] του Google+, η εταιρία συλλέγει δεδομένα θέσης του χρήστη, για τη λειτουργία συναφών υπηρεσιών, όπως η εμφάνιση αναρτήσεων πλησίον του χρήστη, αλλά και για την εξυπηρέτηση των διαφημιστικών υπηρεσιών της Google και των συνεργατών της.

Σε γενικές γραμμές, η κατασκευή του Google+ προσφέρει επαρκή

49 http://www.google.com/intl/en-US/+/policy/

εργαλεία για την προστασία της ιδιωτικότητας των χρηστών και ειδικότερα των στοιχείων θέσης τους, που μας ενδιαφέρουν στο παρόν κείμενο.

Το ζήτημα που τίθεται όμως με το Google+ είναι άλλο: Ειδικά στην περίπτωση της πρόσβασης μέσω φορητής συσκευής Android, πρόκειται για μία μοναδική περίπτωση, γιατί έχουμε τη σύμπτωση των εξής στοιχείων:

Ο δημιουργός του λειτουργικού συστήματος της συσκευής, ο φορέας λειτουργίας του κοινωνικού δικτύου και ο πάροχος των πληροφοριών τοποθεσίας είναι η ίδια η Google.

Πρόκειται για μία μοναδική περίπτωση καθολικής εμπιστοσύνης τόσων προσωπικών δεδομένων σε μία ιδιωτική εταιρία. Και προφανώς τα ερωτήματα ουσιαστικής προστασίας της ιδιωτικότητας που τίθενται είναι πολλά. Τα ερωτήματα μάλιστα πολλαπλασιάζονται αν λάβουμε υπ' όψη και την αλλαγή της πολιτικής δεδομένων[50] των υπηρεσιών της Google την 1η Μαρτίου 2012, που της δίνει ουσιαστικά ένα καθολικό δικαίωμα χρήσης των προσωπικών δεδομένων του χρήστη που διακινούνται μέσω των υπηρεσιών αυτών για διαφημιστικούς κυρίως σκοπούς.

Παρατηρήσεις, ελλείψεις και ευάλωτα χαρακτηριστικά

Η προστασία που παρέχεται στους χρήστες φορητών συσκευών iOS και Android που συνδέονται σε κοινωνικά δίκτυα είναι ελλιπής. Εκτός από ζητήματα που αναφέρθηκαν και άπτονται της προσέγγισης του κάθε λειτουργικού στο θέμα της αποκάλυψης της τοποθεσίας (π.χ το iOS επιτρέπει την εκ των

50 https://www.google.gr/intl/el/policies/privacy/

υστέρων αλλαγή της έγκρισης πρόσβασης στα στοιχεία τοποθεσίας ενώ το Android όχι), παρατηρούμε τα εξής:

α. Ένας χρήστης δεν μπορεί να καθορίσει την ακρίβεια αποκάλυψης της τοποθεσίας του. Δεν έχουν όλες οι υπηρεσίες και εφαρμογές την ίδια ανάγκη γνώσης της τοποθεσίας του χρήστη για να λειτουργήσουν λυσιτελώς. Για παράδειγμα μια υπηρεσία πρόγνωσης καιρού απαιτεί τη γνώση της τοποθεσίας με ακρίβεια δεκάδων χιλιομέτρων, ενώ μια υπηρεσία κλήσης ταξί (π.χ. η εφαρμογή TaxiBeat[51], που επιτρέπει την κλήση ταξί μέσω κινητού) απαιτεί ακρίβεια σε επίπεδο ταχυδρομικής διεύθυνσης. Παρ' όλα αυτά, τα iOS και Android ακολουθούν μια προσέγγιση "όλα ή τίποτα": Αν σε μια εφαρμογή επιτραπεί η πρόσβαση στα στοιχεία εντοπισμού, τότε ο ακριβέστερος εντοπισμός που μπορεί να πετύχει η συσκευή αξιοποιείται.

β. Ακόμη κι αν ο χρήστης απενεργοποιήσει όλα τα συστήματα εντοπισμού όταν εισέρχεται σε μια περιοχή εντός της οποίας επιδιώκει τη βέλτιστη προστασία της θέσης του, υπάρχουν τεχνικές που μπορούν με ακρίβεια να υπολογίσουν την τροχιά του και να προσεγγίσουν τη θέση του (Reid 1979[52], Bayir, Demirbas et al 2009[53])

γ. Τίθεται ένα σημαντικό ζήτημα εμπιστοσύνης του χρήστη στο λειτουργικό σύστημα. Ανά πάσα στιγμή, αν δεν έχουν απενεργοποιηθεί όλες οι λειτουργίες εντοπισμού, το λειτουργικό σύστημα μπορεί να γνωρίζει τη θέση της συσκευής. Ανεξάρτητα από το αν έχει επιτραπεί σε μια υπηρεσία η γνώση της θέσης, το πώς το λειτουργικό σύστημα διαχειρίζεται αυτή τη γνώση είναι εν πολλοίς

51 https://market.android.com/details?id=gr.androiddev.taxibeat&hl=el

52 Reid (1979)

53 Bayir, Demirbas, and Eagle (2009)

άγνωστο. Χαρακτηριστικό είναι το δελτίο τύπου, σε μορφή ερωταποκρίσεων, σχετικά με τη διαχείριση των δεδομένων θέσης, που εξέδωσε η Apple στις 27 Απριλίου 2011,[54] όπου εκτός των άλλων αναγράφεται:

- "Μπορεί η Apple να με εντοπίσει μέσω των καταγεγραμμένων σημείων πρόσβασης WiFi και των δεδομένων των κεραιών κινητής τηλεφωνίας;"

- "Όχι. Τα δεδομένα αυτά αποστέλλονται στην Apple σε ανώνυμη και κρυπτογραφημένη μορφή. Η Apple δεν μπορεί να εντοπίσει την πηγή των δεδομένων"

Κατ' ουσία πρόκειται για μια επίκληση εμπιστοσύνης. Είναι προφανές ότι η από τη στιγμή που ο πάροχος των υπηρεσιών θέσης και αυτός που αιτείται τα δεδομένα θέσης είναι ο ίδιος (εν προκειμένω η Apple), απαιτείται η επίδειξη αυξημένης εμπιστοσύνης από το χρήστη για τη χρήση και αποκάλυψη των δεδομένων αυτών.

δ. Η παροχή σε μια υπηρεσία πρόσβασης στη γνώση της θέσης του χρήστη απαιτεί ομοίως ένα "άλμα πίστης" από την πλευρά του χρήστη. Αυτό προφανώς αφορά οποιαδήποτε ανταλλαγή δεδομένων στο Διαδίκτυο, όπως για παράδειγμα η παροχή των στοιχείων χρέωσης πιστωτικής κάρτας σε ένα ηλεκτρονικό κατάστημα, και εστιάζεται στο δίαυλο μεταφοράς των πληροφοριών (είναι ασφαλής η σύνδεση του site;), στον τρόπο αποθήκευσης αυτών (είναι ασφαλή τα στοιχεία μου από κακόβουλους τρίτους) και στον τρόπο αξιοποίησής τους (ποιοι μαθαίνουν τα στοιχεία μου;). Επιπλέον, οι εταιρίες που παρέχουν υπηρεσίες γεωγραφικού εντοπισμού (απαραίτητες σε

54 http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html

συσκευές που δεν έχουν δέκτη GPS και χρήσιμες ανά περίπτωση σε αυτές που έχουν) είναι ελάχιστες[55] και επομένως όλα αυτά τα δεδομένα τελικά ελέγχονται από λίγους.

ε. Πολλά κοινωνικά δίκτυα παρέχουν μια προγραμματιστική πλατφόρμα, που επιτρέπει σε τρίτους την ανάπτυξη εφαρμογών τρίτων που αξιοποιούν τις υπηρεσίες και τις πληροφορίες του κοινωνικού δικτύου. Αυτό ενδέχεται να εγκυμονεί κινδύνους χρήσης και αξιοποίησης των δεδομένων που γνωρίζει το κοινωνικό δικτύου κατά τρόπο που παραβαίνει την ιδιωτικότητα των μελών του. Πολύ χαρακτηριστικό είναι το παράδειγμα της εφαρμογής "Girls Around Me"[56] για το iOS, που, χρησιμοποιώντας την προγραμματιστική πλατφόρμα του Foursquare, απεικονίζει σε ένα χάρτη, με φωτογραφίες, όλες τις γυναίκες που βρίσκονται πλησίον του χρήστη, επιτρέποντας κατ' ουσία σε κάποιον άγνωστο σε αυτές να τις παρακολουθεί. Εκ των υστέρων το Foursquare απέσυρε από τον κατασκευαστή της εφαρμογής τη δυνατότητα πρόσβασης στην πλατφόρμα του και αιτιολόγησε την απόφασή του υποστηρίζοντας[57] ότι η εφαρμογή χρησιμοποιούσε με μη επιτρεπτό τρόπο το Foursquare, επιχειρώντας την εξαγωγή συγκεντρωτικών στοιχείων (aggregate data) από το λογαριασμό του χρήστη. Ανεξαρτήτως αυτού πάντως, η εν λόγω εφαρμογή απλώς επεξεργαζόταν τα στοιχεία που είναι προσβάσιμα στον οποιοδήποτε χρήστη του Foursquare, αποδεικνύοντας για πολλοστή φορά τον, εκτός του ελέγχου των χρηστών, όγκο των προσωπικών δεδομένων που πολλοί εμπιστεύονται, ακόμα

55 Krontiris, Albers, and Rannenberg (2010)

56 http://girlsaround.me

57 http://news.cnet.com/8301-13772_3-57407384-52/report-foursquare-shuts-off-api-for-girls-around-me-app/

και εν αγνοία τους, στα κοινωνικά δίκτυα.

στ. Με βάση έρευνα της Ευρωπαικής Ένωσης[58], που δημοσιεύτηκε τον Ιούνιο του 2011, παρατηρούμε ότι εννιά στους δέκα Ευρωπαίους θεωρούν ότι η γνωστοποίηση προσωπικών πληροφοριών αποτελεί ολοένα και περισσότερο μέρος της σύγχρονης ζωής. Από την ίδια έρευνα προκύπτει ότι στο πλαίσιο της συμμετοχής σε κοινωνικά δίκτυα, μόλις το 26% των χρηστών του Διαδικτύου πιστεύει ότι έχει τον πλήρη έλεγχο των δεδομένων που αποκαλύπτει. Δηλαδή 3 στους 4 Ευρωπαίους θεωρούν ότι δεν έχουν πλήρη έλεγχο των δεδομένων που αποκαλύπτουν στα κοινωνικά δίκτυα, συμπεριλαμβανομένων των δεδομένων θέσης.

Ως "πλήρη έλεγχο" αντιλαμβανόμαστε τη δυνατότητα ενός χρήστη να:

- να γνωρίζει ανά πάσα στιγμή ποια προσωπικά του δεδομένα έχουν συγκεντρωθεί από τον εκάστοτε φορέα λειτουργίας ενός κοινωνικού δικτύου
- να μπορεί να διαγράψει μέρος ή το σύνολο των δεδομένων αυτών
- να μπορεί να καθορίζει ποια ακριβώς στοιχεία αποκαλύπτει.

Τα αιτήματα αυτά θα πρέπει να ικανοποιούνται χωρίς να χρειάζεται ο χρήστης να κατέχει πολύπλοκες τεχνικές γνώσεις ή να απαιτείται η μελέτη δαιδαλωδών κειμένων για την πολιτική απορρήτου του κάθε παρόχου. Είναι προφανές ότι δεν ικανοποιούνται από την πρακτική του Facebook με τις συνεχείς μεταβολές στην πολιτική απορρήτου του ή το χαρακτηριστικό του Android, μετά από την

58 http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, Τάσεις όσον αφορά την προστασία δεδομένων και την ηλεκτρονική ταυτότητα στην Ευρωπαϊκή Ένωση, Ειδικό Ευρωβαρόμετρο 359

εγκατάσταση μιας εφαρμογής, κατά την οποία ο χρήστης ενημερώνεται για το αν αυτή χρησιμοποιεί τις υπηρεσίας εντοπισμού τοποθεσίας της συσκευής, να μην παρέχεται δυνατότητα απενεργοποίησης της συγκεκριμένης λειτουργίας. ζ. Στην περίπτωση που η πρόσβαση σε ένα κοινωνικό δίκτυο γίνεται μέσω του προγράμματος πλοήγησης του χρήστη στο Διαδίκτυ, τότε θα πρέπει να λάβουμε υπ' όψη την ελλιπή, όσον αφορά την προστασία του χρήση, διαχείριση των δεδομένων τοποθεσίας από τους browsers των εξεταζόμενων λειτουργικών συστημάτων φορητών συσκευών, τα οποία βέβαια συναντάμε ακόμα και στους πιο εξελιγμένους browsers των προσωπικών υπολογιστών. Η έλλειψη άμεσης πληροφόρησης για τη χρήση των δεδομένων τοποθεσίας από τις ιστοσελίδας που τα ζητούν, η ανεπαρκής σήμανση της ενεργοποίησης της έγκρισης, ο ελλιπής εκ των υστέρων έλεγχος των ιστοσελίδων στις οποίες έχει παρασχεθεί έγκριση και η έλλειψη υποχρεωτικής κρυπτογράφησης της επικοινωνίας δεδομένων θέσης[59] συγκαταλλέγονται στα προβλήματα που πρέπει να λύσουν προς την κατεύθυνση της προστασίας των χρηστών οι δημιουργοί των προγραμμάτων πλοήγησης στο Διαδίκτυο.

Ιστορικά στοιχεία

Οι ενστάσεις των χρηστών για τη χρήση των προσωπικών τους δεδομένων από τα κοινωνικά δίκτυα, που επεκτείνεται προφανώς και στο εξεταζόμενο ζήτημα της αποκάλυψης της θέσης του χρήστη, επιτείνονται από τα διάφορα ζητήματα προσβολής της ιδιωτικότητας που έχουν ανακύψει στο

59 Marcos Cáceres, Privacy of Geolocation Implementations, W3C Workshop on Privacy for Advanced Web APIs, 12/13 Ιουλίου 2010, Λονδίνο

παρελθόν.

Ως πιο ενδιαφέροντα και συναφή με τις εταιρίες και τα θέματα που εξετάζονται στο παρόν κείμενο, μπορούμε να αναφέρουμε τα εξής:

Παράκαμψη των ρυθμίσεων ασφαλείας του Safari

Όπως αποκάλυψε[60] στις 17 Φεβρουαρίου του 2012 ο Jonathan Mayer, ερευνητής πρακτικών ασφαλείας του Πανεπιστημίου του Stanford, η Google ενσωμάτωσε σε διαδικτυακές διαφημίσεις κώδικα για την παρακολούθηση των χρηστών του Safari (ο φυλλομετρητής της Apple, που χρησιμοποιείται στο iOS και το OSX). Πιο συγκεκριμένα, ο κώδικας που ενσωματώθηκε είχε ως σκοπό την παράκαμψη των ρυθμίσεων ασφαλείας του Safari, όσον αφορά τη διαχείριση των cookies (μικρά αρχεία κειμένου που δημιουργούνται από τους ιστοτόπους που επισκέπτεται ένας χρήστης στο Διαδίκτυο και αποθηκεύονται στον υπολογιστή του). Όπως διαφημίζει η Apple[61]:

"Πολλές εταιρίες παρακολουθούν τα cookies που δημιουργούνται από τις ιστοσελίδες που επισκέπτεστε, ώστε να συλλέξουν ή και να πουλήσουν πληροφορίες σχετικές με τη δραστηριότητά σας στο Διαδίκτυο. Ο Safari είναι ο πρώτος φυλλομετρητής που μπλοκάρει αυτά τα καταγραφικά cookies εξ ορισμού, προστατεύοντας με τον καλύτερο τρόπο την ιδιωτικότητά σας. Ο Safari αποδέχεται cookies μόνο από τον τρέχοντα τομέα [με τον οποίο επικοινωνεί]".

Η μέθοδος που χρησιμοποίησε η Google, μέσω της διαφημιστικής

60 http://cyberlaw.stanford.edu/blog/2012/02/safari-trackers

61 http://www.apple.com/safari/features.html

τεχνολογίας DoubleClick[62] που έχει αναπτύξει, επέτρεψε, εν αγνοία και παρά τη θέληση του χρήστη, την παράκαμψη αυτής της προστασίας και την αποκάλυψη, τόσο στην Google όσο και σε τρίτους διαφημιζόμενους, των ιστοτόπων που επισκέφτηκε ο χρήστης.

Η Google εξέδωσε ανακοίνωση στην οποία αναγνώριζε την κατάσταση, υποστηρίζοντας όμως ότι η καταγραφή δεν περιείχε προσωπικά στοιχεία και αφορούσε χρήστες που ναι μεν είχαν επιλέξει στις ρυθμίσεις ασφαλείας του Safari να μη καταγράφεται η κίνησή τους στο Διαδίκτυο μέσω cookies, αλλά στις ρυθμίσεις διαφημίσεων των υπηρεσιών της Google είχαν αποδεχτεί την εμφάνιση στο φυλλομετρητής τους διαφημίσεων βασισμένων στις προτιμήσεις τους.

Το ατόπημα αυτό μάλλον έχει τις ρίζες του στον ανταγωνισμό του Google+ με το Facebook για την πρωτοκαθεδρία στο χώρο των κοινωνικών δικτύων. Η Google θέλησε να δημιουργήσει ένα χαρακτηριστικό αντίστοιχο του "Like" του Facebook, και έφτιαξε το "+1" κουμπί – ένα κουμπί που επιτρέπει σε κάθε χρήστη του Google+ να δηλώσει ότι τους αρέσουν διάφορα πράγματα που βλέπει κατά την περιήγησή του στο Διαδίκτυο. Προς το τέλος του 2011 η Google προσέθεσε το κουμπί "+1" στις ηλεκτρονικές διαφημίσεις που προβάλλονται μέσω του συστήματος DoubleClick, θέλοντας να παρακινήσει τους χρήστες για πατάνε το κουμπί για κάθε διαφήμιση που τους αρέσει, ενημερώνοντας έτσι το προφίλ τους στο κοινωνικό δίκτυο για τις προτιμήσεις τους. Αυτή η πρακτική ερχόταν σε σύγκρουση με το σύστημα "Do Not Track" τους Safari κι έτσι οι μηχανικοί της Google εφάρμοσαν το προαναφερθέν

62 http://www.google.com/doubleclick/

σύστημα παράκαμψης, που όπως φαίνεται[63] θα κοστίσει στην εταιρία ένα μεγάλο πρόστιμο.

Η περίπτωση αυτή έχει ιδιαίτερο ενδιαφέρον, παρ' ότι σίγουρα μεγαλοποιήθηκε στην προβολή της, για δύο κυρίως λόγους: Αφ' ενός δείχνει πόσο μεγάλη σημασία έχει για τις εταιρίες, που δραστηριοποιούνται στο χώρο της Διαδικτυακής διαφήμισης, να μπορούν να συλλέγουν στοιχεία για τις συνήθειες των χρηστών, ώστε να μπορούν να παρουσιάζουν συναφέστερες και ακριβέστερες διαφημίσεις, αφ' ετέρου γιατί αποδεικνύει πόσο ευάλωτες και ανεπαρκείς είναι οι εφαρμοζόμενες μέθοδοι προστασίας των προσωπικών δεδομένων ενός χρήστη.

Καταγραφή δεδομένων από το Street View

Το Google Street View[64] είναι ένα προσάρτημα της υπηρεσίας Google Maps, που επιτρέπει την απεικόνιση πανοραμικών φωτογραφιών που λαμβάνονται από δρόμους μεγάλων πόλεων σε διάφορες χώρες. Οι φωτογραφίες λαμβάνονται από ειδικά αυτοκίνητα της εταιρίας που κινούνται στους δρόμους. Πέραν του φωτογραφικού εξοπλισμού, τα αυτοκίνητα αυτά διαθέτουν και εξοπλισμό ασύρματης δικτύωσης, που χρησιμοποιήθηκε για την καταγραφή στοιχείων από παρακείμενα στα αυτοκίνητα ασύρματα δίκτυα, με στόχο τη βελτίωση της βάσης δεδομένων ασύρματων σημείων πρόσβασης της Google (όπως αναφέρθηκε ανωτέρω, στο κεφάλαια "άμεσος εντοπισμός".

63 http://www.bloomberg.com/news/2012-05-04/google-said-to-face-fine-by-u-s-over-apple-safari-breach.html

64 http://maps.google.com/intl/en/help/maps/streetview/

Όπως προέκυψε κατά την έρευνα τον γερμανικών αρχών το Μάιο του 2010, όταν η εταιρία αποφάσισε να επεκτείνει την υπηρεσία και στη Γερμανία,[65] κατά τη λήψη των φωτογραφιών τα αυτοκίνητα της Google συγκέντρωναν αναγνωριστικά στοιχεία για τον εντός εμβέλειας ασύρματο εξοπλισμό, όπως διευθύνσεις MAC και γεωγραφικές συντεταγμένες σημείων πρόσβασης και δρομολογητών, καθώς και μέρος των δεδομένων που διακινούνταν μέσω αυτών – σε κάποιες περιπτώσεις κωδικούς πρόσβασης και μηνύματα ηλεκτρονικού ταχυδρομείου.

Ο θόρυβος και οι αντιδράσεις που προκλήθηκαν από την αποκάλυψη ήταν το έναυσμα για μια μεγάλη συζήτηση στη Γερμανία σχετικά με τα όρια της ιδιωτικότητας. Ένα από τα αποτελέσματα της συζήτησης ήταν ότι περί τους 245.000 ανθρώπους κατέθεσαν αίτηση στην Google για τον αποκλεισμό της διεύθυνσης κατοικίας ή εργασίας τους από τη φωτογράφηση.[66]

Η ίδια πρακτική στη Γαλλία, οδήγησε τη Γαλλική Αρχή Προστασίας Δεδομένων (CNIL) να επιβάλει πρόστιμο 100.000 ευρώ στη Google και να απαιτήσει από την εταιρία τη δημοσιοποίηση όλων των ενεργειών της που σχετίζονται με την επεξεργασία προσωπικών δεδομένων, συμπεριλαμβανομένων των δεδομένων τοποθεσίας από την υπηρεσία Google Latitude.[67]

65 http://news.bbc.co.uk/2/hi/technology/8684110.stm

66 http://www.time.com/time/world/article/0,8599,2100051,00.html

67 http://www.cnil.fr/la-cnil/actu-cnil/article/article/street-view-la-cnil-met-en-demeure-google-de-lui-communiquer-les-donnees-wi-fi-enregistrees/

Καταγραφή κινήσεων από το iOS

Τον Απρίλιο του 2011 οι ανεξάρτητοι ερευνητές Alasdair Allan και Pete Warden ανακοίνωσαν[68] ότι οι συσκευές με iOS, από την έκδοση 4.0 και μετά, αποθηκεύουν στη συσκευή ένα αρχείο, που περιλαμβάνει γεωγραφικές συντεταγμένες και χρονοσημάνσεις (timestamps) για τις τοποθεσίες που έχει επισκεφθεί ο χρήστης της συσκευής. Οι καταγεγραμμένες τοποθεσίας δεν χρησιμοποιούν το δέκτη GPS της συσκευής για τον ακριβή εντοπισμό της, αλλά τις θέσεις των ανά πάσα στιγμή συνδεδεμένων με αυτήν σταθμών κινητής τηλεφωνίας.

Το αρχείο, με την ονομασία consolidated.db, είναι αποθηκευμένο σε μη κρυπτογραφημένη μορφή στη συσκευή και παρ' ότι, από την έρευνα, δεν προέκυψε ότι τα περιεχόμενά του αποστέλλονταν σε τρίτους, η παρουσία του γέννησε πολλά ερωτηματικά. Προς τι η ύπαρξη του αρχείου; Γιατί η καταγραφή γινόταν εν αγνοία των χρηστών; Η Apple ανακοίνωσε ότι το αρχείο δημιουργείται για να επιτρέπει στη συσκευή να εντοπίζει πιο γρήγορα τη θέση της όταν δεν υπάρχει σύνδεση με δορυφόρο GPS ή σημείο πρόσβασης WiFi.[69]

Τα στοιχεία που αποκαλύπτει το αρχείο είναι, ούτως ή άλλως, γνωστά στους παρόχους κινητής τηλεφωνίας, αλλά η αποκάλυψή τους γινόταν μόνο κατόπιν εισαγγελικής ή δικαστικής παραγγελίας. Η παρουσία του στο iOS επιτρέπει σε οποιονδήποτε έχει στην κατοχή του τη φορητή συσκευή και πρόσβαση σε έναν υπολογιστή ή και μόνο τη συσκευή, αν σε αυτή έχει εφαρμοστεί το jailbreak (παράκαμψη των δικλείδων ασφαλείας της Apple για

68 http://radar.oreilly.com/2011/04/apple-location-tracking.html
69 http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html

την εγκατάσταση μη εγκεκριμένου λογισμικού), να εξάγει τα αποθηκευμένα δεδομένα και να δημιουργήσει ένα πλήρες προφιλ κίνησης του χρήστη της συσκευής. Προς απόδειξη αυτού, ο Peter Warden δημιούργησε μια εφαρμογή[70] που απεικονίζει όλες τις αποθηκευμένες τοποθεσίες σε ένα χάρτη.

Οι ανωτέρω καταγεγραμμένες περιπτώσεις δημόσιου προβληματισμού για τις πρακτικές προστασίας απορρήτου της Google και της Apple, φέρνουν στην επιφάνεια την ουσία του προβλήματος:

Ανεξάρτητα απ' το πόσο διακυβεύεται το προσωπικό απόρρητο ενός χρήστη από το consolidated.db ή τις φωτογραφίες του Google Street View ή τις στοχευμένες διαφημίσεις για τους χρήστες Safari, η πραγματικότητα είναι πως:

- τα προσωπικά δεδομένα έχουν τεράστια οικονομική αξία
- οι δυνατότητες διασύνδεσης και εντοπισμού που ενσωματώνουν τα σύγχρονα κινητά τηλέφωνα και οι άλλες συναφείς φορητές συσκευές μπορούν να συστήσουν ουσιαστικό κίνδυνο για τα προσωπικό δεδομένα των χρηστών
- οι εταιρείες, στις οποίες καλούνται οι χρήστες να εμπιστευτούν τα δεδομένα τους, έχουν ένα ιστορικό που δημιουργεί, λιγότερο ή περισσότερο δικαιολογημένη, καχυποψία

Το ισχύον νομικό πλαίσιο

Οι κοινωνικές προεκτάσεις και επιπτώσεις των θεμάτων προστασίας προσωπικών δεδομένων που ανακύπτουν από τη χρήση φορητών συσκευών

70 http://petewarden.github.com/iPhoneTracker/

προφανώς έχει απασχολήσει και τη νομοθεσία. Στο πλαίσιο της Ευρωπαικής Ένωσης και επομένως και στην Ελλάδα, μπορούμε να διακρίνουμε τη προστασία των προσωπικών δεδομένων θέσης[71] σε ειδική και γενική.

Ειδική προστασία

Η ειδική προστασία αναφέρεται αυτοτελώς στα δεδομένα θέσης, βάσει την επεξεργασία δεδομένων σταθμών βάσης (κεραίες κινητής τηλεφωνίας, σημείο πρόσβασης WiFi) και διακρίνει την εφαρμογή της έναντι των φορέων εκμετάλλευσης τηλεπικοινωνιών και των φορέων παροχής υπηρεσιών της κοινωνίας της πληροφορίας.

Φορείς εκμετάλλευσης τηλεπικοινωνιών

Στην πρώτη περίπτωση εφαρμόζεται η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (2002/58/ΕΚ, όπως αναθεωρήθηκε από την οδηγία 2009/136/ΕΚ) και ισχύει μόνο για την επεξεργασία δεδομένων σταθμών βάσης από δημόσια δίκτυα και φορείς εκμετάλλευσης τηλεπικοινωνιών.

Οι φορείς εκμετάλλευσης τηλεπικοινωνιών υποβάλλουν διαρκώς σε επεξεργασία δεδομένα σταθμών βάσης στο πλαίσιο της παροχής των υπηρεσιών τους. Σε αυτή τη δραστηριότητα συμπεριλαμβάνεται και η παροχή δημόσιων σημείων πρόσβασης WiFi από παρόχους τηλεπικοινωνιακών υπηρεσιών.

71 Γνώμη 13/2011 σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών, 16 Μαίου 2011, WP 185.

Μπορούν επίσης να επεξεργάζονται δεδομένα προκειμένου να παρέχουν υπηρεσίες προστιθέμενης αξίας.[72]

Στις δραστηριότητες αυτές, η οδηγία 2002/58/ΕΚ, της 12ης Ιουλίου 2002 (όπως αναθεωρήθηκε τον Νοέμβριο του 2009 από την οδηγία 2009/136/ΕΚ), είναι εφαρμοστέα, σύμφωνα με τον ορισμό που προβλέπεται στο άρθρο 2 στοιχείο γ) της εν λόγω οδηγίας: Ως «δεδομένα θέσης» νοούνται τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Ο φορέας εκμετάλλευσης τηλεπικοινωνιών πρέπει να διασφαλίζει την εκ των προτέρων συγκατάθεση των πελατών του σε περίπτωση που κοινοποιεί τα συγκεκριμένα δεδομένα γεωγραφικής θέσης σε τρίτους.

Από τη στιγμή που τα δεδομένα θέσης που προέρχονται από σταθμούς βάσης συνδέονται με φυσικό πρόσωπο κατονομαζόμενο ή του οποίου η ταυτότητα μπορεί να εξακριβωθεί, εμπίπτουν στις διατάξεις που διέπουν τη γενική προστασία δεδομένων προσωπικού χαρακτήρα, όπως προβλέπονται στην οδηγία 95/46/ΕΚ,της 24ης Οκτωβρίου 1995 (βλπ. παρακάτω – υπό τον τίτλο "γενική προστασία")

Φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας

Στην περίπτωση των φορέων παροχής υπηρεσιών της κοινωνίας της

72 Γνώμη 5/2005 της Ομάδας Εργασίας του άρθρου 29 για τη χρήση δεδομένων θέσης με σκοπό την παροχή υπηρεσιών προστιθέμενης αξίας, 25 Νοεμβρίου 2005, WP 115.

πληροφορία, συνήθως, οι εταιρείες που παρέχουν υπηρεσίες και εφαρμογές εντοπισμού θέσης με βάση συνδυασμό δεδομένων σταθμών βάσης, GPS και WiFi είναι υπηρεσίες της κοινωνίας της πληροφορίας και, ως εκ τούτου, εξαιρούνται ρητώς από τον σαφή ορισμό των υπηρεσιών ηλεκτρονικών επικοινωνιών της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.[73] Στις περιπτώσεις αυτές, εφαρμόζεται η γενική οδηγία 95/46/ΕΚ.

Γενική προστασία

Όπως προαναφέρθηκε, το οικείο νομικό πλαίσιο της γενικής προστασίας προστασίας δεδομένων προσωπικού χαρακτήρα είναι η οδηγία 95/46/ΕΚ[74]. Με βάση αυτή, δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί (το πρόσωπο στο οποίο αναφέρονται τα δεδομένα)· ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή
κοινωνική άποψη —άρθρο 2 στοιχείο α) της οδηγίας.

73 Οδηγία 2002/21/ΕΚ, της 7ης Μαρτίου 2002, άρθρο 2 στοιχείο γ.

74 Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

Οι αιτιολογικές σκέψεις 26 και 27 της οδηγίας, καθώς και η γνώμη 4/2007 μας επιτρέπουν να διαπιστώσουμε το πεδίο εφαρμογής της στα δεδομένα θέσης:

Η αιτιολογική σκέψη 26 της οδηγίας εστιάζει στον όρο «μπορεί να εξακριβωθεί», με τη φράση «για να διαπιστωθεί αν η ταυτότητα ενός προσώπου μπορεί να εξακριβωθεί, πρέπει να λαμβάνεται υπόψη το σύνολο των μέσων που μπορούν ευλόγως να χρησιμοποιηθούν, είτε από τον υπεύθυνο της επεξεργασίας, είτε από τρίτο, για να εξακριβωθεί η ταυτότητα του εν λόγω προσώπου.»

Η αιτιολογική σκέψη 27 της οδηγίας σκιαγραφεί το ευρύ πεδίο εφαρμογής της προστασίας: «το πεδίο εφαρμογής της προστασίας αυτής δεν πρέπει πράγματι να εξαρτάται από τις χρησιμοποιούμενες τεχνικές, δεδομένου ότι αυτό θα δημιουργούσε σοβαρούς κινδύνους καταστρατήγησης».

Στη γνώμη 4/2007 σχετικά με την έννοια του όρου δεδομένα προσωπικού χαρακτήρα, η ομάδα εργασίας παρέσχε εκτενή καθοδήγηση για τον ορισμό των δεδομένων προσωπικού χαρακτήρα και για τη σύνδεσή τους με τα δεδομένα θέσης. Η γνώμη αναγνωρίζει την άρρηκτη σύνδεση μιας "έξυπνης" φορητής συσκευής με ένα φυσικό πρόσωπο, με βάση:

- τα αρχεία του παρόχου κινητής τηλεφωνίας, που περιέχουν το όνομα, τη διεύθυνση και άλλα μοναδικά αναγνωριστικά του συνδρομητή (π.χ. ΑΦΜ)
- τα μοναδικά διακριτικά της συσκευής, όπως τους αριθμούς IMEI (διεθνής αναγνωριστικός αριθμός εξοπλισμού κινητής τηλεφωνίας) και IMSI (διεθνής ταυτότητα κινητού συνδρομητή)

- τη σύνδεση με τα ανωτέρω στοιχεία άμεσα αναγνωρίσιμων οικονομικών δεδομένων κατά τη αγορά πρόσθετου λογισμικού για τη συσκευή μέσω πιστωτικής κάρτας
- το συνδυασμό τεχνολογιών που μπορούν να εντοπίσουν με ακρίβεια τη θέση του

Αυτή η εξέλιξη διευκολύνει τη σύνδεση ενός προτύπου θέσης ή συμπεριφοράς με συγκεκριμένο άτομο και εντάσσονται στην κατηγορία των προσωπικών δεδομένων, ακόμη και στην περίπτωση που όνομα του χρήστη δεν είναι γνωστό, γιατί, βάσει των μοναδικών στοιχείων αναγνώρισης που περιγράφονται, τον καθιστούν "διακριτό".

Επιπλέον, η έμμεση εξακρίβωση του φυσικού προσώπου ισχύει επίσης και για τα σημεία πρόσβασης WiFi. Το γεγονός ότι σε ορισμένες περιπτώσεις ο κάτοχος της συσκευής επί του παρόντος δεν μπορεί να προσδιοριστεί χωρίς την καταβολή υπέρμετρης προσπάθειας, δεν επηρεάζει το γενικό συμπέρασμα ότι τα δεδομένα του σημείου πρόσβασης WiFi και της εκτιμώμενης θέσης του θα πρέπει να εκλαμβάνονται ως δεδομένα προσωπικού χαρακτήρα.

Υπενθυμίζεται σε αυτό το σημείο ότι για την εφαρμογή της διάταξης δεν είναι απαραίτητο η επεξεργασία των συγκεκριμένων δεδομένων γεωγραφικής θέσης να επιδιώκει ή να καταλήγει στον εντοπισμό των χρηστών. Ο βαθμός της προσπάθειας που απαιτείται για τον εντοπισμό των κατόχων των σημείων πρόσβασης WiFi εξαρτάται σε μεγάλο βαθμό από τις τεχνικές δυνατότητες του υπευθύνου της επεξεργασίας δεδομένων ή άλλου προσώπου που είναι επιφορτισμένο με τον εντοπισμό τους.

Υποχρεώσεις που απορρέουν από τη νομοθεσία

Με βάση όσα προαναφέρθηκαν, δηλαδή την οδηγία της ΕΕ για την προστασία των δεδομένων (95/46/ΕΚ) και την αναθεωρημένη Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, καθώς και τις ερμηνευτικές γνώμες που αναφέρονται σε αυτές, προκύπτουν διαφορετικές υποχρεώσεις για τα διάφορα ενδιαφερόμενα μέρη, που καλύπτουν από σχεδιαστές λειτουργικών συστημάτων έως παρόχους εφαρμογών, καθώς και τρίτους όπως δικτυακούς τόπους κοινωνικής δικτύωσης που ενσωματώνουν στις πλατφόρμες τους λειτουργικές δυνατότητες εντοπισμού θέσης για κινητές συσκευές.

Τα δεδομένα θέσης που προκύπτουν από έξυπνες κινητές συσκευές είναι δεδομένα προσωπικού χαρακτήρα. Ο συνδυασμός των μοναδικών διευθύνσεων MAC και της εκτιμώμενης θέσης του σημείου πρόσβασης WiFi θεωρούνται επίσης δεδομένα προσωπικού χαρακτήρα.

Οι υπεύθυνοι επεξεργασίας των δεδομένων θέσης διαχωρίζονται στις ακόλουθες τρεις κατηγορίες: υπεύθυνοι των υποδομών εντοπισμού γεωγραφικής θέσης (συγκεκριμένα υπεύθυνοι της επεξεργασίας των χαρτογραφημένων σημείων πρόσβασης WiFi), πάροχοι εφαρμογών και υπηρεσιών εντοπισμού γεωγραφικής θέσης και σχεδιαστές λειτουργικών συστημάτων έξυπνων κινητών συσκευών.

Για την επεξεργασία των δεδομένων, πρέπει οι υπεύθυνοι αυτής να έχουν θεμιτό λόγο επεξεργασίας. Επειδή τα δεδομένα θέσης των έξυπνων

κινητών συσκευών αποκαλύπτουν προσωπικές πληροφορίες σχετικά με την ιδιωτική ζωή του κατόχου της συσκευής, το βασικό στοιχείο για τη νόμιμη επεξεργασία είναι η συγκατάθεση κατόπιν ενημέρωσης. Η συγκατάθεση δεν είναι εφικτό να αποσπάται μέσω γενικών όρων και προϋποθέσεων. Η συγκατάθεση πρέπει να αφορά τον εκάστοτε συγκεκριμένο σκοπό επεξεργασίας των δεδομένων από τον υπεύθυνο της επεξεργασίας, όπως για παράδειγμα την κατάρτιση προφίλ και/ή την εξειδικευμένη αντιμετώπιση με βάση τη συμπεριφορά. Σε περίπτωση που οι σκοποί της επεξεργασίας τροποποιηθούν κατά τρόπο ουσιώδη, ο υπεύθυνος της επεξεργασίας πρέπει να ζητήσει την εκ νέου συγκατάθεση.

Κατά την αγορά της συσκευής, οι υπηρεσίες εντοπισμού θέσης πρέπει να είναι απενεργοποιημένες. Μηχανισμοί εξαίρεσης δεν αποτελούν επαρκείς μηχανισμούς για τη λήψη της συγκατάθεσης του χρήστη κατόπιν ενημέρωσης.

Η συγκατάθεση στο εργασιακό πλαίσιο και σε παιδιά είναι προβληματική. Όσον αφορά τους εργαζομένους, οι εργοδότες μπορούν να χρησιμοποιούν τη συγκεκριμένη τεχνολογία μόνο εφόσον είναι αποδεδειγμένα αναγκαία για θεμιτό σκοπό και οι ίδιοι στόχοι δεν μπορούν να επιτευχθούν με λιγότερο παρεμβατικό τρόπο. Όσον αφορά τα παιδιά, οι γονείς είναι αυτοί που κρίνουν αν η χρήση της εν λόγω συσκευής είναι αιτιολογημένη υπό συγκεκριμένες συνθήκες. Οφείλουν τουλάχιστον να ενημερώνουν τα παιδιά τους και να τους επιτρέπουν να συμμετέχουν στην απόφαση για τη χρήση των εν λόγω εφαρμογών το νωρίτερο δυνατό.

Η "Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα", γνωστή και ως "Ομάδα του Άρθρου 29",

που συστήθηκε δυνάμει του άρθρου 29 της Οδηγίας 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, συνιστά τον περιορισμό του φάσματος της συγκατάθεσης όσον αφορά τη διάρκεια της επεξεργασίας και την υπενθύμιση των χρηστών τουλάχιστον σε ετήσια βάση. Η ομάδα εργασίας συνιστά επίσης τον επαρκή επιμερισμό της συγκατάθεσης όσον αφορά τον βαθμό ακρίβειας των δεδομένων θέσης.

Στα υποκείμενα των δεδομένων πρέπει να παρέχεται η δυνατότητα εύκολης ανάκλησης της συγκατάθεσής τους, χωρίς αυτό να επιφέρει αρνητικές συνέπειες στη χρήση της συσκευής τους.

Όσον αφορά τη χαρτογράφηση των σημείων πρόσβασης WiFi, οι εταιρείες δύνανται να έχουν έννομο συμφέρον στην αναγκαία συλλογή και επεξεργασία των διευθύνσεων MAC και των εκτιμώμενων θέσεων των σημείων πρόσβασης WiFi για συγκεκριμένους σκοπούς παροχής υπηρεσιών εντοπισμού γεωγραφικής θέσης. Για τη στάθμιση των συμφερόντων μεταξύ των δικαιωμάτων του υπευθύνου επεξεργασίας και των δικαιωμάτων των υποκειμένων των δεδομένων, ο υπεύθυνος της επεξεργασίας πρέπει να παρέχει δικαίωμα εύκολης και μόνιμης εξαίρεσης από τη βάση δεδομένων, χωρίς να απαιτείται η κοινοποίηση πρόσθετων δεδομένων προσωπικού χαρακτήρα.

Τρίτοι, όπως προγράμματα περιήγησης στο διαδίκτυο (web browsers) και δικτυακοί τόποι κοινωνικής δικτύωσης διαδραματίζουν βασικό ρόλο όσον αφορά την ορατότητα και την ποιότητα των πληροφοριών σχετικά με την επεξεργασία δεδομένων γεωγραφικής θέσης.

Οι διάφοροι υπεύθυνοι επεξεργασίας των πληροφοριών γεωγραφικής

θέσης από κινητές συσκευές θα πρέπει να παρέχουν στους πελάτες τη δυνατότητα να αποκτούν πρόσβαση στα δεδομένα θέσης, σε μορφή αναγνώσιμη από άνθρωπο και να παρέχουν επίσης τη δυνατότητα διόρθωσης και διαγραφής χωρίς να απαιτείται συλλογή υπερβολικών δεδομένων προσωπικού χαρακτήρα.

Επίσης θα πρέπει να διασφαλίζουν ότι οι κάτοχοι έξυπνων κινητών συσκευών είναι επαρκώς ενημερωμένοι σχετικά με τα βασικά στοιχεία της επεξεργασίας σύμφωνα με το άρθρο 10 της οδηγίας για την προστασία των δεδομένων. Στα στοιχεία αυτά περιλαμβάνονται μεταξύ άλλων, η ταυτότητα του υπευθύνου της επεξεργασίας, οι σκοποί της επεξεργασίας, τα είδη των δεδομένων, η διάρκεια της επεξεργασίας, τα δικαιώματα των υποκειμένων των δεδομένων στην πρόσβαση, διόρθωση ή ακύρωση των δεδομένων τους και το δικαίωμα ανάκλησης της συγκατάθεσης.

Οι πληροφορίες πρέπει να είναι σαφείς, περιεκτικές, κατανοητές για το ευρύ κοινό χωρίς εξειδικευμένες τεχνικές γνώσεις και να είναι εύκολα προσβάσιμες επί μονίμου βάσεως. Η εγκυρότητα της συγκατάθεσης είναι άρρηκτα συνδεδεμένη με την ποιότητα των πληροφοριών σχετικά με την υπηρεσία.

Τα υποκείμενα των δεδομένων διατηρούν επίσης το δικαίωμα πρόσβασης, διόρθωσης και διαγραφής πιθανών προφίλ που καταρτίζονται με βάση τα εν λόγω δεδομένα θέσης.

Η ομάδα εργασίας συνιστά στους υπευθύνους της επεξεργασίας να αναζητούν ασφαλείς τρόπους για την παροχή άμεσης επιγραμμικής πρόσβασης σε δεδομένα θέσης και ενδεχόμενα προφίλ. Η πρόσβαση τέτοιου τύπου πρέπει

να είναι εφικτή χωρίς την παροχή πρόσθετων δεδομένων προσωπικού χαρακτήρα.

Βάσει της Οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ[75], οι πάροχοι κινητής τηλεφωνίας και πρόσβασης Διαδικτύου υποχρεούνται να διατηρούν δεδομένα που μπορούν να προσδιορίσουν ατομικά χρήστες (όπως μηνύματα ηλεκτρονικού ταχυδρομείου, δεδομένα θέσης, αναγνωριστικά ταυτότητας κυψέλης κινητής τηλεφωνίας κλπ) για μια χρονική περίοδο από έξι μήνες έως δύο έτη. Αντίστοιχα, οι πολιτικές διατήρησης των δεδομένων που εφαρμόζονται από τους παρόχους εφαρμογών ή υπηρεσιών εντοπισμού γεωγραφικής θέσης θα πρέπει να διασφαλίζουν ότι τα δεδομένα γεωγραφικής θέσης ή τα προφίλ που καταρτίζονται με βάση αυτά τα δεδομένα, διαγράφονται ύστερα από εύλογο χρονικό διάστημα.

Αν ο σχεδιαστής του λειτουργικού συστήματος και/ή ο υπεύθυνος των υποδομών εντοπισμού γεωγραφικής θέσης υποβάλλει σε επεξεργασία μοναδικό αριθμό, όπως διεύθυνση MAC ή UDID σχετικά με δεδομένα θέσης, ο μοναδικός αριθμός ταυτοποίησης μπορεί να αποθηκεύεται για μέγιστο διάστημα 24 ωρών για λειτουργικούς σκοπούς, καθ' ότι η υποχρέωση διατήρησης δεδομένων δεν τους βαρύνει ούτε και τους απαλλάσσει από την υποχρέωση προστασίας.

75 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:el:HTML

Η ανωτέρω περιγραφείσα νομοθεσία της Ευρωπαικής Ένωσης συντάχθηκε το 1995, σε μια εποχή που η διείσδυση της τεχνολογίας στην καθημερινή ζωή ήταν σαφώς μικρότερη. Παρά την αναθεώρηση με την Οδηγία 2002/58/ΕΚ, έχει κριθεί ότι πλέον δεν είναι επαρκής και, όπως θα δούμε παρακάτω, η Ευρωπαική Επιτροπή επεξεργάζεται την αλλαγή του νομικού αυτού πλαισίου.

Ποιοι τρόποι προστασίας προτείνονται

Η πληθώρα των τρόπων με τους οποίους μπορεί να αποκαλυφθεί η τοποθεσία ενός χρήστη, οδηγούν και σε πληθώρα εφαρμοζόμενων ή προτεινόμενων μεθόδων επίλυσης του προβλήματος. Οι λύσεις που προτείνονται είτε προσπαθούν με αλγοριθμικές μεθόδους και εργαλεία λογισμικού να προστατεύσουν τη θέση των χρηστών και να τους αποδώσουν μεγαλύτερο έλεγχο για την αποκάλυψη της θέσης τους, είτε εστιάζουν στο νομικό επίπεδο, και ελέγχουν την πολιτική και τις πρακτικές απορρήτου της εκάστοτε υπηρεσίας.

Αλγοριθμικές μέθοδοι

Οι περισσότερες αλγοριθμικές μέθοδοι προστασίας εστιάζουν κυρίως σε περιπτώσεις συνεχούς παρακολούθησης της θέσης του χρήστη, που γίνεται σε κοινωνικά δίκτυα όπως το Foursquare και σε υπηρεσίας όπως το Google Latitude ή το Facebook Places.

Ανωνυμία

Πολλοί συγγραφείς έχουν προσεγγίσει το πρόβλημα ως ζήτημα εξασφάλισης της ανωνυμίας του χρήστη, υπό την έννοια τη μη αναγνώρισης της ταυτότητας ενός χρήστη μέσα σε ένα σύνολο.

```
επίσκεψηΠροστατευμένηςΠεριοχής = ΟΧΙ
Σε κάθε ενημέρωση θέσης {
      Αν η νέα θέση υπάγεται σε νέα ζώνη {
            αν ΟΧΙ επίσκεψηΠροστατευμένηςΠεριοχής {
                  Αποκάλυψε διαδρομή
            }
            Διάγραψε διαδρομή
            επίσκεψηΠροστατευμένηςΠεριοχής = ΟΧΙ
            Αποκάλυψε τη νέα ζώνη
      }
      Πρόσθεσε τρέχουσα τοποθεσία σε διαδρομή
      Αν η τρέχουσα θέση εντός προστατευμένης περιοχής {
            επίσκεψηΠροστατευμένηςΠεριοχής = ΝΑΙ
      }
}
```

Εικόνα 9: Ο αλγόριθμος k-area: Όλες οι ενημερώσεις τοποθεσίας σε μία ζώνη καταγράφονται και δεν αποκαλύπτονται, παρά μόνο αν ο χρήστης περάσει σε άλλη ζώνη. Αν η προηγούμενη ζώνη ήταν από τις προστατευμένες, τότε οι ενημερώσεις τοποθεσίας αυτής της ζώνης αποκρύπτονται, ειδάλλως αποκαλύπτονται. Η διαδικασία επαναλαμβάνεται για κάθε ζώνη που έχει επισκεφθεί ο χρήστης.

Οι Gruteser M. & Liu X. στο Protecting Privacy in Continuous Location -

Tracking Applications προτείνουν την ορισμό περιοχών υψηλής προστασίας των δεδομένων θέσης εντός των οποίων δεν θα γίνεται προβολή της θέσης από τη φορητή συσκευή. Οι θέσεις αυτές ορίζουν ένα "χάρτη ευαισθησίας", βάσει του οποίου κρίνεται αν η συσκευή θα πρέπει να αποκαλύψει τη θέση της στην ενδιαφερόμενη υπηρεσία. Για τη βέλτιστη αποκάλυψη της θέσης, ώστε και η βασισμένη στη γνώση της θέσης υπηρεσία (LBS) να λειτουργεί σωστά αλλά και να μη διακυβεύεται η αποκάλυψη της θέσης του χρήστη, όσο αυτός βρίσκεται εντός των ζωνών υψηλής προστασίας, προτείνουν και αξιολογούν τρεις αλγόριθμους αποκάλυψης: base, bounded rate και k-area. Ο base αλγόριθμος συνιστά την απλή προσέγγιση, βάσει της οποίας η συσκευή προβαίνει σε αποκάλυψη της θέσης της, αν αυτή είναι εκτός των προστατευμένων περιοχών του χάρτη. Η λύση αυτή προσφέρει μικρή προστασία, γιατί επιτρέπει την εξαγωγή συμπερασμάτων για τη θέση του χρήστη εντός των προστατευμένων περιοχών, λαμβάνοντας υπ' όψη τα σημεία εισόδου σε αυτές.

Ο bounded rate αλγόριθμος φροντίζει ώστε η συχνότητα των αποκαλύψεων θέσης να είναι χαμηλότερη από ένα προκαθορισμένο κατώφλι – με αυτόν τον τρόπο εξασφαλίζεται, ανάλογα με το κατώφλι, μεγαλύτερη πιθανότητα να μην αποκαλύπτεται η θέση στα όρια του χάρτη εμπιστευτικότητας.

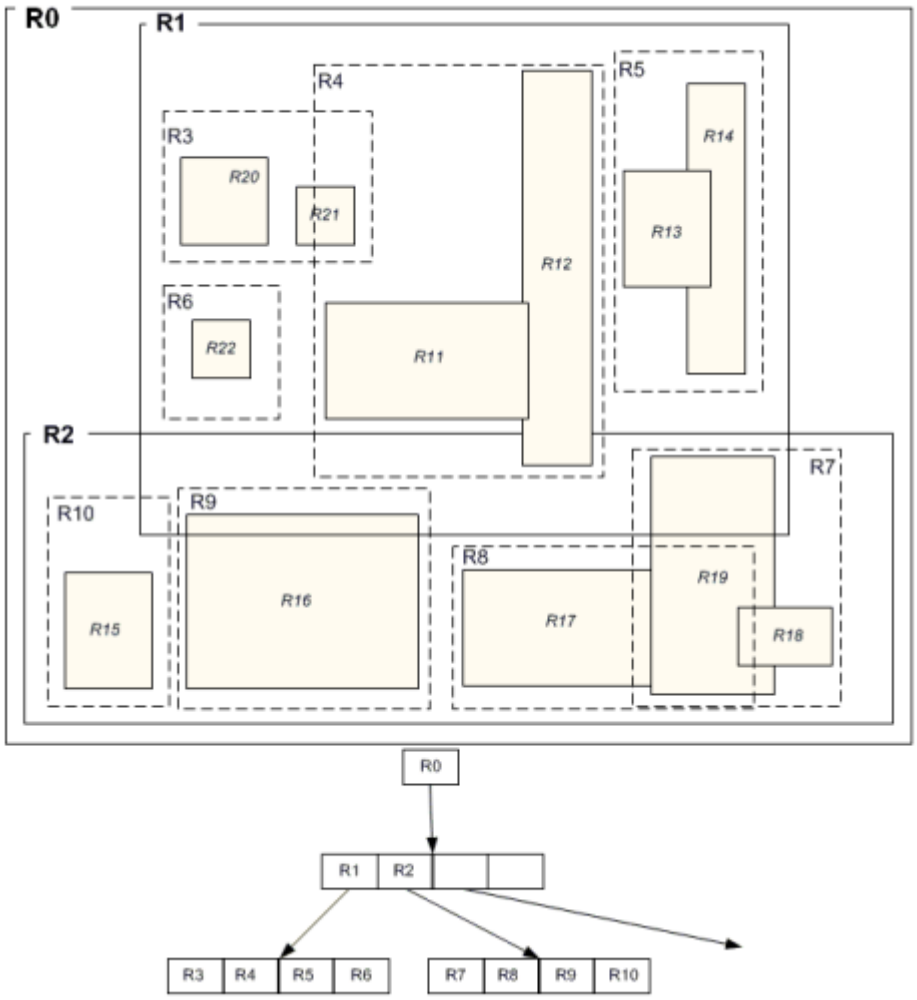
Ο k-area αλγόριθμος εξασφαλίζει ότι εκτός των προστατευμένων περιοχών, η προβολή της θέσης θα γίνεται μόνο αν δεν επιτρέπει την αποκάλυψη τουλάχιστον k περιοχών υψηλής προστασίας. Για να επιτευχθεί αυτό, ο χάρτης ευαισθησίας χωρίζεται σε ζώνες, που περιέχουν κατ' ελάχιστον k διακριτές ευαίσθητες περιοχές. Ως "διακριτή ευαίσθητη περιοχή" ορίζουμε μια

περιοχή στην οποία μπορεί κανείς να φτάσει ερχόμενος από μια δημόσια (= μη προστατευόμενη) περιοχή και από την οποία δεν μπορούμε να εισέλθουμε σε άλλη ευαίσθητη περιοχή χωρίς να περάσουμε από μία δημόσια περιοχή. Για παράδειγμα, κάθε κτίριο σε ένα οικοδομικό τετράγωνο συνιστά διακριτή ευαίσθητη περιοχή, γιατί η είσοδος σε αυτό γίνεται από το δρόμο (δημόσια περιοχή) και δεν είναι δυνατόν να περάσουμε σε άλλο κτίριο χωρίς να βγούμε στο δρόμο.[76]

Αξιολογώντας τους αλγόριθμους, οι συγγραφείς κατέληξαν στο συμπερασμα ότι ο base αλγόριθμος προσφέρει ελάχιστη προστασία, όπως και ο bounded-rate, αν ορίσουμε μεγάλη συχνότητα ενημερώσεων. Αν στον bounded-rate ορίσουμε μικρή συχνότητα, τότε μειώνεται η ακρίβεια ενημέρωσης στις δημόσιες περιοχές. Ο k-area προσφέρει αποτελεσματική προστασία, αλλά καθυστερεί την αποστολή ενημερώσεων μέχρι ο χρήστης να φύγει από μια προστατευμένη περιοχή. Αναγνωρίζουν τέλος ότι ακόμα κι αν επιτευχθεί επαρκής προστασία προς την κατεύθυνση της ανωνυμίας, στοιχεία όπως η συχνότητα επίσκεψης μιας προστατευμένης περιοχής ή η διάρκεια παραμονής σε αυτήν μπορούν επίσης να διακυβεύσουν την ιδιωτικότητα ενός χρήστη.

Οι Gruteser και Grunwald προτείνουν ένα μοντέλο, όπου οι φορητές συσκευές θα εκπέμπουν ενημερώσεις τοποθεσίας μέσα από έναν έμπιστο server, που θα εξασφαλίζει ότι η προς αποκάλυψη τοποθεσία θα περιέχει τουλάχιστον k-1 άλλους χρήστες (k-ανωνυμία). Για το σκοπό αυτό, αξιολογούν τη χρήση από το server (anonymizer) ενός αλγόριθμου απόκρυψης

76 Gruteser and Liu (2004)



Εικόνα 10: Γραφική αναπαράσταση του adaptive-interval cloaking αλγόριθμου. Στο παράδειγμα, υποθέτουμε ότι οι κόμβοι R13, R14, R11, R12, R8, R9, R10 περιέχουν έναν χρήστη. Αν kmin = 5 και ο προστατευμένος χρήστης βρίσκεται στο R11, ο αλγόριθμος χωρίζει τοπεδίο εφαρμογής σε υποπεριοχές, μέχρι τη στιγμή που φτάνει στο R4, που περιέχει λιγότερα από 5 άτομα. Τότε επιστρέφει την περιοχή R1, που είναι η αμέσως προηγούμενη που καλύπτει το kmin.

προσαρμοσμένου διαστήματος (adaptive-interval cloaking algorithms). Η βασική ιδέα του αλγορίθμου αυτού είναι ότι ένας βαθμός ανωνυμίας μπορεί να επιτευχθεί σε οποιαδήποτε περιοχή, ανεξάρτητα από το πλήθος των αντικειμένων που βρίσκονται σε αυτήν, μειώνοντας την ακρίβεια της τοποθεσίας που αποκαλύπτεται. Φυσικά, αν κριτήριο είναι η μεγαλύτερη ακρίβεια της αποκάλυψης τοποθεσίας, τότε ο ορισμός των περιοχών πρέπει να γίνεται έχοντας ως κριτήριο και την πλήθος των αντικειμένων τους.

Το επιθυμητό επίπεδο ανωνυμίας οριζεται από την παράμετρο k_{min}, που περιέχει το ελάχιστο αποδεκτό μέγεθος του συνόλου ανωνυμίας. Επιπλέον, ο αλγόριθμος λαμβάνει ως είσοδο την τρέχουσα θέση του χρήστη φορητής συσκευής που θέλει να προστατεύσει τη θέση του (L), τα όρια της περιοχής που ελέγχει ο anonymizer και τη θέση των άλλων αντικειμένων στην ίδια περιοχή. Με αυτά τα στοιχεία, χωρίζει αναδρομικά την περιοχή σε υποπεριοχές, ώστε το σύνολο των ατόμων που βρίσκονται στην ίδια περιοχή να είναι κάτω από το όριο k_{min} και τελικά επιστρέφει την υποπεριοχή στην οποία βρίσκονται οι συντεταγμένες εισόδου L.

Τα βήματα του αλγόριθμου παρουσιάζονται ως εξής:

1. Όρισε τα τεταρτημόρια (υποπεριοχές) q και q_{prev} ώστε να καλύπτουν όλη τη ζώνη ευθύνης του anonymizer.
2. V = σύνολο όλων των θέσεων χρηστών στην περιοχή
3. L = θέση χρήστη προς απόκρυψη
4. Αν οι χρήστες στο V < k_{min}, τότε επίστρεψε υποπεριοχή q_{prev}
5. Χώρισε το q σε ισοδύναμες υποπεριοχές
6. q_{prev} = q

7. q = υποπεριοχή που περιέχει το L
8. Απομάκρυνε όλες τις θέσεις εκτός q από το V
9. Πήγαινε στο βήμα 2

Στην εικόνα 10 φαίνεται μια γραφική παράσταση της εκτέλεσης του αλγορίθμου.[77]

Μια αντίστοιχη προσέγγιση στην απόκρυψη τοποθεσίας είναι η χρονική απόκρυψη. Αυτή η μέθοδος μπορεί να αποκαλύψει με μεγαλύτερη ακρίβεια τη θέση, μειώνοντας τη χρονική ακρίβεια. Η βασική τεχνική είναι η καθυστέρηση της αποκάλυψης της θέσης L1 μέχρις ότου k_{min} χρήστες εισέλθουν στην ίδια υποπεριοχή. Στην περίπτωση αυτή, ο χωρισμός σε υποπεριοχές δεν θα γίνεται βάσει του k_{min}, αλλά βάσει μιας επιπλέον παραμέτρου εισόδου. Ο anonymizer θα παρακολουθεί την είσοδο χρηστών στην προς αποκάλυψη υποπεριοχή και όταν ο αριθμός αυτών φτάσει το k_{min}, τότε υπολογίζεται ένα χρονικό διάστημα *[t1, t2]* ως εξής: Το *t2* τίθεται στη στιγμή εισόδου του k_{min} ατόμου στην υποπεριοχή και το *t1* στη στιγμή αποκάλυψης της θέσης L1 πλην μια τυχαία τιμή απόκρυψης. Η υποπεριοχή και το *[t1, t2]* επιστρέφονται από τον αλγόριθμο.[78]

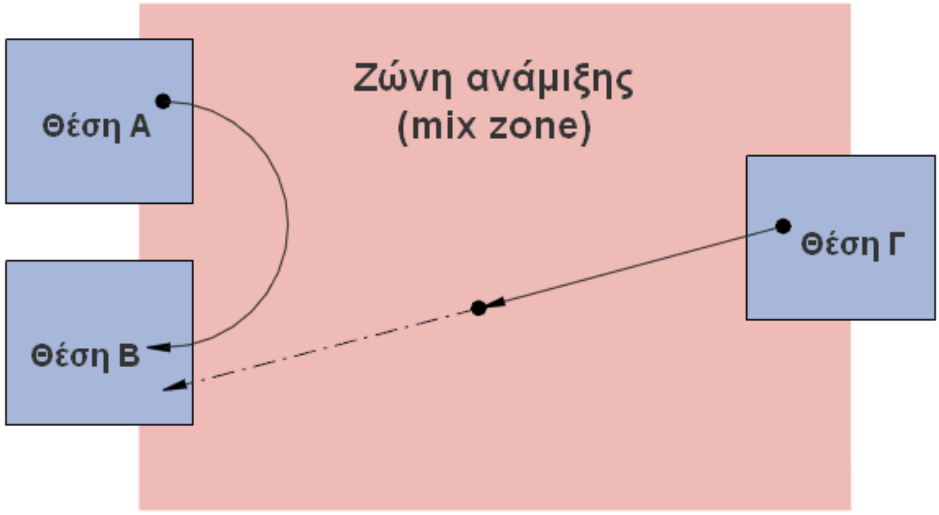
Οι Beresford και Stajano, σε μια άλλη προσέγγιση στην k-ανωνυμία, βασισμένοι στην εργασία του David Chaum στον τομέα της ανώνυμης επικοινωνίας,[79] εισάγουν τη χρήση των *ζωνών ανάμιξης* (mix zones). Πρόκειται

77 Όπως την παρουσιάζουν Nayot Poolsappasit και Indrakshi Ray στο "Towards Achieving Personalized Privacy for Location-Based Services"

78 Gruteser and Grunwald (2003)

79 D. Chaum, "Untraceable Electronic Mail, Return Addresses and Digital

για ζώνες εντός των οποίων δεν γίνεται αποκάλυψη από φορητές συσκευές της θέσης τους. Οι ζώνες αυτές ορίζονται κατά τέτοιο τρόπο, ώστε να μην είναι δυνατή η ταυτοποίηση των φορητών συσκευών που έχουν εισέλθει, από διάφορες θέσεις εισόδου, σε αυτές.[80] Για το σκοπό αυτό, Οι συγγραφείς εφαρμόζουν το μοντέλο τους σε σε περιπτώσεις υπηρεσιών βασισμένων στην τοποθεσία (location-based services – LBS) που μπορούν να χρησιμοποιηθούν με ψευδώνυμο, δηλαδή δεν έχουν αυστηρά προσωπικό χαρακτήρα, και



Εικόνα 11: Παράδειγμα διάταξης μιας ζώνης ανάμιξης. Οι θέσεις Α και Β είναι πιο κοντά απ' ότι οι θέση Γ. Χρήστες που εισέρχονται την ίδια στιγμή στη ζώνη ανάμιξης, προερχόμενοι από τη θέση Α και τη θέση Γ, δεν θα διακρίνονται όταν εισέλθουν στη θέση Β.

Pseudonyms," Comm. ACM, vol. 24, no. 2, 1981, σελ. 84–88.

80 Beresford and Stajano (2003)

συνδυάζεται με τη συνεχή αλλαγή ψευδωνύμων κατά την είσοδο σε μια ζώνη ανάμιξης. Επιπλέον η επικοινωνία της συσκευής του χρήστη με την υπηρεσία δεν γίνεται απ' ευθείας, αλλά μέσω ενός *μεσολαβητή ανωνυμίας* (anonymity proxy).

Οι Kido et al εξετάζουν την αναφορά ψευδών θέσεων μαζί με την αναφορά της αληθινής θέσης και εν συνεχεία την αξιοποίηση μόνο της ανταπόκρισης στην αναφορά της αληθινής θέσης από την υπηρεσία τοποθεσίας. Στην έρευνά τους προτείνουν τρόπους για τη προώθηση αληθοφανών ψευδών θέσεων και για την ελάττωση των επιπτώσεων της αναπόφευκτης επιπλέον επικοινωνίας με τον πάροχο πληροφοριών θέσης. Ορίζουν ως βασικούς άξονες της επίτευξης ανωνυμίας την *πανταχού παρουσία* (ubiquity), τη *συμφόρηση* (congestion) και την *ομοιομορφία* (uniformity) των θέσεων των χρηστών, όπου:

- πανταχού παρουσία: σε όλο το χώρο εφαρμογής του μοντέλου θα πρέπει να βρίσκονται χρήστες
- συμφόρηση: θα πρέπει να συναντάται πλήθος ατόμων στις υποπεριοχές του χώρου εφαρμογής
- ομοιομορφία: η κατανομή των ατόμων στις διάφορες υποπεριοχές θα πρέπει να είναι περίπου ίση

Βάσει του μοντέλου τους, ο χρήστης αποστέλλει στην υπηρεσία τοποθεσίας ένα μήνυμα:

S = (u, L_1, L_2,... , L_m)

όπου το u είναι το αναγνωριστικό του χρήστη και (L_1, L_2,... , L_m) είναι δεδομένα

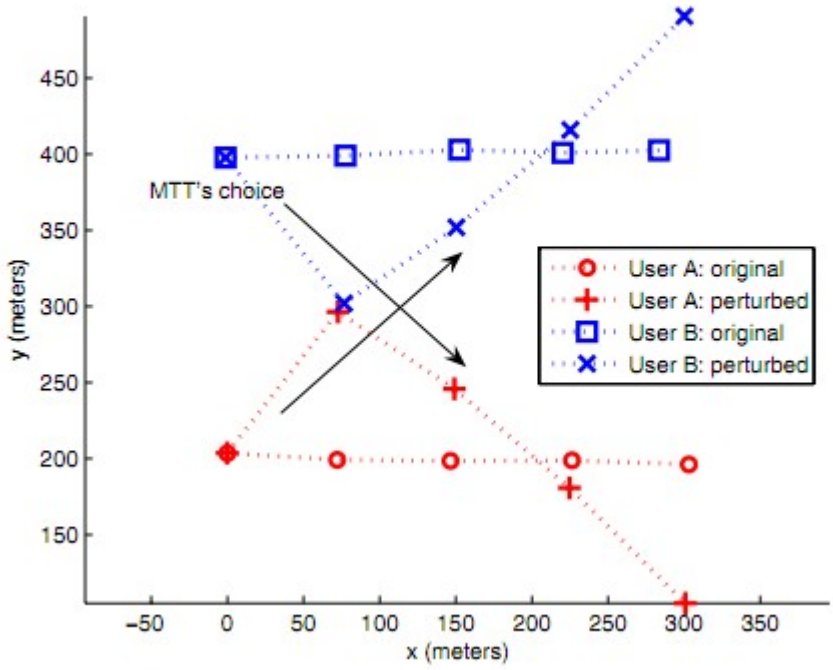
θέσης, εκ των οποίων το ένα είναι αληθές και τα m-1 ψευδή. Η υπηρεσία απαντά με το μήνυμα:

$$\mathbf{R} = ((L_1,D_1),(L_2,D_2),...,(L_m,D_m))$$

Ο χρήστης μπορεί να αντιστοιχίσει στην αληθή θέση L_i την απάντηση D_i, οπότε το πρόβλημα μετακυλίεται στη δημιουργία αληθοφανών ψευδών στοιχείων, από τα οποία να μην μπορεί να εξαχθεί η πραγματική θέση του χρήστη και ταυτόχρονα να μην είναι εύκολη η απόρριψή τους ως ψευδών. Για το σκοπό αυτό οι συγγραφείς προτείνουν δύο αλγόριθμους, τον Moving in a Neighborhood (MN) και τον Moving in a Limited Neighborhood (MNM). Και στους δύο αλγόριθμους η πρώτη ψευδής θέση που αποστέλλεται βρίσκεται πλησίον της πραγματικής θέσης. Με τον αλγόριθμο MN η επόμενη ψευδής θέση προς αποστολή υπολογίζεται εντός της περιοχής της προηγούμενης ψευδούς θέσης, δηλαδή η συσκευή του χρήστη καταγράφει τις ψευδείς θέσεις που έχουν αποσταλεί και τοποθετεί τις επόμενες πλησίον της τελευταίας θέσης. Με τον αλγόριθμο MNM, η επόμενη ψευδής θέση είναι ομοίως στη "γειτονιά" της προηγούμενης, αλλά λαμβάνεται επιπλέον υπόψη το κριτήριο της θέσης άλλων χρηστών εντός της ίδιας περιοχής. Αν υπάρχουν περισσότεροι χρήστες, τότε η ψευδής θέσης επαναυπολογίζεται, δημιουργώντας σύγχυση και σε σχέση με τις θέσεις των άλλων χρηστών. Αξιολογώντας την επίτευξη της προστασίας της θέσης, το αλγοριθμικό κόστος όσο και την οικονομία εύρους ζώνης κατά την πρακτική εφαρμογή του αλγόριθμου, οι συγγραφείς καταλήγουν εκτιμώντας ότι ο αλγόριθμος μπορεί να εφαρμοστεί και σε πραγματικές συνθήκες.[81]

81 Kido, Yanagisawa, and Satoh (2005)

Άλλες μέθοδοι



Εικόνα 12: Γραφική παράσταση του αλγόριθμου διαταραχής τροχιών των Gruteser και Hoh. Οι Α και Β κινούνται σε παράλληλες τροχιές, αλλά ο αλγόριθμος τις μεταβάλει σε τροχιές που τέμνονται. ώστε να προκαλέσει τη σκοπούμενη σύγχυση.

Στο ίδιο πλαίσιο της επιδίωξης ανωνυμίας, η τεχνική της διαταραχής τροχιών (path perturbation)[82] που προτείνουν οι Gruteser και Hoh προκαλεί σύγχυση των τροχιών που τέμνονται, ώστε να αποτύχει η ταυτοποίηση της

82 Baik Hoh and Gruteser (2005)

κάθε τροχιάς, άρα και θέσης, με τη χρήση αλγορίθμων εντοπισμού πολλαπλών στόχων (Multi-Target Tracking[83]). Ο αλγόριθμος που προτείνουν οι συγγραφείς επιτυγχάνει διαταραχή των τροχιών μέσω της μεταβολής των αναφερθεισών θέσεων δύο χρηστών που βρίσκονται σε κοντινή απόσταση μεταξύ τους. Αυτή η τεχνική μειώνει το χρόνο για τον οποίο κάποιος κακόβουλος τρίτος θα μπορούσε να παρακολουθήσει ένα άτομο και πετυχαίνει, βάσει των πειραματικών δεδομένων κυκλοφορίας οχημάτων που χρησιμοποίησαν οι συγγραφείς, επαρκή προστασία χωρίς να μειώνει ουσιωδώς την ακρίβεια των αποκαλύψεων θέσης. Λόγω της φύσης του υπόκειται σε περιορισμούς, όσον αφορά την πυκνότητα ατόμων στο χώρο εφαρμογής. Αν η πυκνότητα είναι μικρή, τότε θα πρέπει να θυσιαστεί ουσιωδώς η ακρίβεια των δεδομένων. Στην εικόνα 11 φαίνεται μια γραφική παράσταση εφαρμογής του αλγόριθμου.

Οι Zhong et al[84] προσεγγίζουν το πρόβλημα "του κοντινού φίλου", δηλαδή της εύρεσης σε ένα κοινωνικό δίκτυο συσχετισμένων μελών που βρίσκονται στην ίδια περιοχή. Για την προστασία των δεδομένων θέσης, προτείνουν τρία διαφορετικά πρωτόκολλα επικοινωνίας και αποκάλυψης της θέσης, στα οποία εφαρμόζουν κρυπτογραφία δημοσίου κλειδιού. Τα προτεινόμενα πρωτόκολλα τα ονομάζουν Louis, Lester και Pierre.[85] Από αυτά, το πιο πρόσφορο για την αντιμετώπιση του προβλήματος είναι το Louis, γιατί το Pierre δεν αποκαλύπτει την ακριβή απόσταση από τον κοντινό φίλο, ενώ το Lester την αποκαλύπτει, αλλά ενέχει το ενδεχόμενη της αποκάλυψης της θέσης

83 Reid (1979)

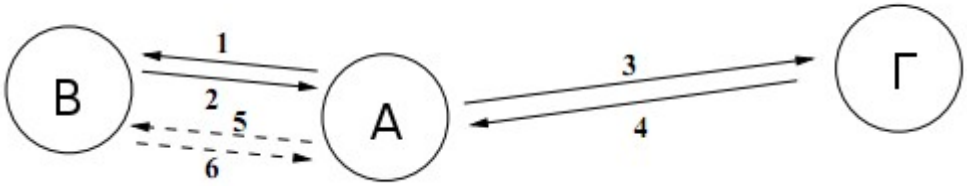
84 Zhong, Goldberg, and Hengartner (2007)

85 Η εφαρμογή NearByFriend (http://crysp.uwaterloo.ca/software/nearbyfriend/) είναι μια υλοποίηση του πρωτοκόλλου Pierre.

ενός χρήστη, παρ' ότι αυτός έχει μετακινηθεί εκτός της ζητούμενης εμβέλειας. Στο πρωτόκολλο Louis συμμετέχουν τρία μέρη, τα Α, Β και Γ. Τα Α και Β είναι οι δύο φίλοι, εκ των οποίων ο Α εκκινεί τη διαδικασία και ο Β ανταποκρίνεται, ενώ το μέρος Γ λειτουργεί ως ημιέμπιστος μεσάζοντας επικοινωνίας. Η επικοινωνία γίνεται σε δύο φάσεις: στην πρώτη ο Α επικοινωνεί με τον Β στέλνοντας κρυπτογραφημένα στοιχεία για τη θέση του και τη ζητούμενη ακτίνα εντός της οποίας αναζητά τον Β, ο Β ανταποκρίνεται (αν αποδεχτεί τη ζητούμενη ακτίνα και δεν τη θεωρήσει υπερβολικά μεγάλη) στέλνοντας κρυπτογραφημένα με το δημόσιο κλειδί του Γ στοιχεία στον Α, αυτός τα μεταδίδει στον Γ ο οποίος, χωρίς να γνωρίζει την ταυτότητα του Β και την ακτίνα, αποκρίνεται για τον αν η θέση του είναι εντός της ζητούμενης από τον Α εμβέλειας. Στη δεύτερη φάση, που είναι προαιρετική και εκτελείται αν κριθεί από την πρώτη ότι οι Α και Β είναι κοντά, αποκαλύπτεται η ακριβής θέση του ενός στον άλλο.

Η επικοινωνία μεταξύ των μερών γίνεται μέσω ασφαλών καναλιών και κρυπτογραφείται χρησιμοποιώντας το σύστημα Paillier,[86] μια τεχνική κρυπτογράφησης που επιτρέπει την εφαρμογή αλγεβρικών πράξεων στη μη κρυπτογραφημένη τιμή, εφαρμόζοντας μια πράξη στην κρυπτογραφημένη τιμή. Αν η πράξη είναι πρόσθεση, τότε η τεχνική καλείται "προσθετική ομομορφική κρυπτογράφηση" (additive homomorphic encryption). Η χρήση του συστήματος Paillier επιτρέπει στον Γ να μπορεί να κάνει υπολογισμούς και να λάβει αποτελέσματα χωρίς να γνωρίζει τις αρχικές τιμές.

86 P. Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, Advances in Cryptology-Eurocrypt '99, σελ. 223-238.



Εικόνα 13: Γραφική αναπαράσταση των βημάτων επικοινωνίας του πρωτοκόλλου Louis. Η διακεκομμένη γραμμή δείχνει την προεραιτική, δεύτερη φάση.

Οι Gupta et al ανέλυσαν το πρωτόκολλο Louis, παρατήρησαν ότι είναι ευάλωτο στην περίπτωση που δύο από τα εμπλεκόμενα μέρη ψεύδονται για τη θέση τους και πρότειναν την εφαρμογή ενός πρωτοκόλλου "αποκοπής και επιλογής" (cut and choose protocol) κατά την επικοινωνία του Α με τον Γ. Βάσει αυτού, ο Α στέλνει μια σειρά μηνυμάτων στον Γ, εκ των οποίων μόνο ένα αναφέρεται στις τιμές που έχει λάβει από τον Β, ενώ τα υπόλοιπο κατασκευάζονται έτσι, ώστε ο Α να γνωρίζει τη σωστή απάντηση. Ο Γ αποκρίνεται σε όλα τα μηνύματα απαντώντας αν βρίσκονται εντός της ζητούμενης θέσης και ο Α, λαμβάνοντας τις απαντήσεις, γνωρίζει ποια απάντηση ανταποκρίνεται στην ερώτηση βάσει πραγματικών στοιχείων και ποιες στις υπόλοιπες. Αν τα κατασκευασμένα μηνύματα έχουν την αναμενόμενη απάντηση, τότε η μόνη περίπτωση να ψεύδεται ο Γ και στην περίπωση της πραγματικής ερώτησης ισχύσει στην περίπτωση που μπορέσει, τυχαία, να "μαντέψει" ποιο από τα επιλεγμένα μηνύματα του Α είναι πραγματικό, δηλαδή

για την αποστολή Ν μηνυμάτων οι πιθανότητας είναι 1/Ν. Αν οι απαντήσεις του Γ είναι οι αναμενόμενες, τότε, αν αποδειχτεί λάθος κατά την αξιολόγηση του πρωτοκόλλου, το λάθος/ψεύδος προέρχεται από τον Β. Όπως σημειώνουν και οι συγγραφείς, αυτή η λύση δεν μπορεί να θεωρηθεί επαρκής, τόσο λόγω του πιθανολογικού χαρακτήρα της, όσο και λόγω της επιβάρυνσης της επικοινωνίας μεταξύ των μερών με επιπλέον μηνύματα.[87]

Οι Krontiris et el εισάγουν μια άλλη προσέγγιση ελέγχου απευθείας στη φορητή συσκευή[88]. Συγκεκριμένα, προτείνουν τη δημιουργία μιας εφαρμογής/διεργασίας παρασκηνίου που θα καταγράφει τις πληροφορίες θέσης που αποστέλλονται από τη φορητή συσκευή και θα παρατηρούν (monitor όπως το ονομάζουν) αν διακυβεύεται η ιδιωτικότητα του χρήστη, βάσει των προκαθορισμένων προτιμήσεών στις δεδομένες συνθήκες χρήσεις. Για παράδειγμα όταν ο χρήσης βρίσκεται στο σπίτι του μπορεί να επιθυμεί πλήρη απόκρυψη των πληροφοριών θέσης του, ενώ στο χώρο εργασίας του μπορεί να επιτρέπει την ανά ημίωρο προβολή της θέσης του. Η διεργασία παρατήρησης θα ενημερώνει το χρήστη αν επίκειται μη επιτρεπτή διαρροή τοπικών πληροφοριών, επιτρέποντάς του να την απαγορεύσει. Πρόκειται κατ' ουσία για ένα παραμετροποιημένο κατά συνθήκες τείχος προστασίας εξερχομένων τοπικών πληροφοριών (context sensitive outbound firewall for location data). Δεν έχει προταθεί κάποια συγκεκριμένη υλοποίηση της εν λόγω ιδέας, αλλά ενδέχεται να συνιστά ένα χρήσιμο επικουρικό μέσο προστασίας.

Οι Friedland & Sommer[89] προσεγγίζουν με διαφορετικό τρόπο το

87 Security analysis of the Louis protocol for location privacy (2009)

88 Krontiris, Albers, and Rannenberg (2010)

89 Friedland and Sommer (2010)

Εικόνα 14: Η πρόταση των Friedland & Sommer για τον ορισμό της ακρίβειας geotagging φωτογραφιών

πρόβλημα, επιδιώκοντας να επαυξήσουν τον παρεχόμενο στο χρήστη έλεγχο της αποκάλυψης της θέσης του. Εστιάζουν στο ζήτημα του Geotagging και προτείνουν τη διαβάθμιση της ακρίβειας αποκάλυψης της θέσης κατά τις επιλογές του χρήστη. Ως παράδειγμα, παρουσιάζουν ένα προτεινόμενο παράθυρο διαλόγου του iOS, στο οποίο ο χρήστης μπορεί να επιλέξει αν θέλει να καταγράψει την τοποθεσία λήψης μιας φωτογραφίας με ακρίβεια ακριβούς διεύθυνσης κατοικίας, οικοδομικού τετραγώνου, πόλης, ευρύτερης περιοχής ή χώρας (εικόνα 13). Οι συγγραφείς προτείνουν επίσης μια εναλλακτική προσέγγιση, βάσει της οποίας συγκεκριμένες πολιτικές απορρήτου θα εφαρμόζονται κατά την αποστολή φωτογραφιών σε κοινωνικά δίκτυα ή εν γένει δημοσίως προσβάσιμους διαδικτυακούς χώρους. Αντί δηλαδή να ελέγχεται κατά τη λήψη μιας φωτογραφίας αν θα καταγραφεί στα μεταδεδομένα της η

τοποθεσία λήψης, αυτό θα ελέγχεται κατά τη διαδικασία αποστολής, οπότε και ο χρήστης θα ερωτάται αν επιθυμεί τη συμπερίληψη των μεταδεδομένων. Επίσης, θα μπορούσε να μετακυλιστεί το βάρος μείωσης της ακρίβειας αποκάλυψης στην προγραμματιστική πλατφόρμα που παρέχουν διάφορες υπηρεσίας, όπως το Flickr και το YouTube.

Πολιτικές απορρήτου

Ο Kaasinen[90] προτείνει την αξιοποίηση και επέκταση του πρωτοκόλλου P3P ώστε να περιλαμβάνει και τα δεδομένα θέσης. Το P3P (Πρόγραμμα Πλατφόρμας για τις Επιλογές Ιδιωτικότητας - Platform for Privacy Preferences Project) αναπτύχθηκε[91] από το World Wide Web Consortium (W3C) και ορίζει μια μέθοδο περιγραφής των προσωπικών πληροφοριών που συλλέγει κάθε ιστοσελίδα. Με τη μέθοδο αυτή το πρόγραμμα περιήγησης του χρήστη στο Διαδίκτυο μπορεί να συγκρίνει την πολιτική ασφαλείας της ιστοσελίδας με τις προκαθορισμένες επιλογές του χρήστη και ανάλογα με την περίπτωση, να αποδεχτεί τη μεταφορά δεδομένων, να την αποτρέψει ή να ενημερώσει το χρήστη. Το δημοσιευμένο πρότυπο του P3P (v1.0) δεν συμπεριλαμβάνει τα δεδομένα θέσης στις προδιαγραφές του. Σε κάθε περίπτωση, το P3P συνιστά μια απλή σύσταση και δεν έχει δεσμευτικό χαρακτήρα.

Η Ευρωπαική Ένωση εξέδωσε στις 25-1-2012 ανακοίνωση[92], με την οποία προωθεί τη μεταρρύθμιση του καθεστώτος προστασίας δεδομένων, ώστε

90 Kaasinen (2003)

91 http://www.w3.org/TR/P3P/

92 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

να μπορέσει να συμβαδίσει με τις τεχνολογικές εξελίξεις και τα πραγματικά προβλήματα προστασίας που ανακύπτουν, στο βαθμό που αυτά δεν μπορούν να καλυφθούν από την ισχύουσα Οδηγία 95/46ΕΚ. Ειδικά οι ιστότοποι κοινωνικής δικτύωσης και οι βασισμένες στη θέση υπηρεσίες (Location based Services – LBS) αναφέρονται επακριβώς στο κείμενο που διαγράφει τους άξονες της μεταρρύθμισης:[93]

> *Πρέπει επίσης να εκσυγχρονιστούν οι ισχύοντες κανόνες οι οποίοι θεσπίστηκαν όταν το Διαδίκτυο έκανε ακόμη τα πρώτα του βήματα. Η ταχεία τεχνολογική πρόοδος και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις όσον αφορά την προστασία δεδομένων. Με τους ιστότοπους κοινωνικής δικτύωσης, τα υπολογιστικά νέφη, τις υπηρεσίες εντοπισμού θέσης (LBS) και τις έξυπνες κάρτες, αφήνουμε ψηφιακά ίχνη με κάθε κίνησή μας. Σε αυτόν τον «θαυμαστό νέο κόσμο δεδομένων» χρειαζόμαστε ένα ισχυρό σύνολο κανόνων.*
>
> *Η μεταρρύθμιση του καθεστώτος προστασίας δεδομένων θα διασφαλίσει τη βιωσιμότητα και την καταλληλότητα των κανόνων μας για την ψηφιακή εποχή.*

Οι βασικοί άξονες που προτείνονται και σχετίζονται με την προστασία των δεδομένων θέσης αποτυπώνονται στα εξής:

- Η καθιέρωση ενός νέου «δικαιώματος στη λήθη» θα βοηθήσει τα άτομα στην καλύτερη διαχείριση των κινδύνων που κρύβει το διαδίκτυο για την

93 http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

προστασία δεδομένων. Όταν κάποιος δεν επιθυμεί πλέον την επεξεργασία των δεδομένων του και εφόσον δεν συντρέχουν νόμιμοι λόγοι για τη διατήρησή τους, τα δεδομένα θα διαγράφονται.

- Όταν απαιτείται συγκατάθεση για τη διαχείριση δεδομένων, αυτή θα πρέπει να δίδεται ρητά, και όχι να λαμβάνεται ως δεδομένη.
- Διευκόλυνση της πρόσβασης των χρηστών στα δεδομένα τους και θέσπιση του δικαιώματος φορητότητας δεδομένων, δηλαδή διευκόλυνση τη μεταφοράς προσωπικών δεδομένων από έναν πάροχο υπηρεσιών σε άλλον.
- Οι εταιρείες και οι οργανισμοί θα υποχρεούνται να γνωστοποιούν σοβαρές παραβιάσεις δεδομένων χωρίς καθυστέρηση, και, εφόσον είναι εφικτό, εντός 24 ωρών.
- Ενιαίο σύνολο κανόνων για την προστασία δεδομένων, οι οποίοι θα ισχύουν σε όλη την ΕΕ.
- Οι εταιρείες θα είναι υπόλογες σε μία μόνο εθνική αρχή προστασίας δεδομένων στη χώρα της ΕΕ στην οποία έχουν την έδρα τους.
- Τα άτομα θα έχουν δικαίωμα να αναφέρουν όλες τις υποθέσεις στην εθνική αρχή προστασίας δεδομένων της χώρας τους, ακόμη και αν τα προσωπικά δεδομένα τους υποβάλλονται σε επεξεργασία εκτός της χώρας τους.
- Οι κανόνες της ΕΕ εφαρμόζονται σε εταιρείες μη εγκατεστημένες στην ΕΕ, εφόσον αυτές παρέχουν εμπορεύματα ή υπηρεσίες στην ΕΕ ή παρακολουθούν τη διαδικτυακή συμπεριφορά πολιτών της Ένωσης.
- Αυξημένη ευθύνη και υποχρέωση λογοδοσίας για όσους επεξεργάζονται

δεδομένα προσωπικού χαρακτήρα.

- Οι περιττές διοικητικές επιβαρύνσεις, όπως π.χ. οι απαιτήσεις κοινοποίησης για τις εταιρείες που επεξεργάζονται προσωπικά δεδομένα, θα καταργηθούν.
- Θα ενισχυθούν οι εθνικές αρχές προστασίας δεδομένων ώστε να είναι σε θέση να επιβάλλουν πιο αποτελεσματικά τους κανόνες της ΕΕ στην εκάστοτε χώρα. ατόμων, ενδυνάμωση της εσωτερικής αγοράς της ΕΕ, διασφάλιση υψηλού επιπέδου προστασίας των δεδομένων σε όλους τους τομείς συμπεριλαμβανομένης της αστυνομικής και της δικαστικής συνεργασίας σε ποινικές υποθέσεις, διασφάλιση της αποτελεσματικής επιβολής των κανόνων και καθιέρωση παγκόσμιων προτύπων για την προστασία δεδομένων.

Τα ανωτέρω σημεία δεν έχουν ακόμα συγκροτηθεί σε Οδηγία, αλλά βρίσκονται στο επίπεδο των προπαρασκευαστικών συζητήσεων και προτάσεων. Από τη μελέτη τους όμως διαφαίνονται κάποιες σημαντικές τάσεις, που η νομοθεσία είχε παραβλέψει ως τώρα: Επιδιώκεται η μεταβίβαση μεγαλύτερου ελέγχου στα προσωπικά δεδομένα των χρηστών, συμπεριλαμβανομένης της δυνατότητας πρόσβασης σε αυτά και γνώσης της χρήσης του μετά από τη γνωστοποίησή τους. Λαμβάνεται υπ' όψη ο διακρατικός χαρακτήρας του Διαδικτύου και τονίζεται η ανάγκη ενίσχυσης της εμπιστοσύνης των χρηστών στο Διαδίκτυο, ώστε να δοθεί ώθηση στη σχετική, αποκλειστική ή επικουρική διαδικτυακή επιχειρηματικότητα.

Η ENACSO[94] (European NGO Alliance for Child Safety Online) – Ευρωπαική Συμμαχία Μη Κυβερνητικών Οργανώσεων για την Προστασία των Παιδιών στο Διαδίκτυο), προτείνει[95] τη δημουργία μιας ανεξάρτητας αρχής έγκρισης, στην κρίση της οποίας θα τίθεται η λειτουργία εφαρμογών που χρησιμοποιούν τεχνολογίες εντοπισμού. Για την έγκριση της εφαρμογής θα απαιτείται ο έλεγχος ότι οι προσωπικές πληροφορίες που συλλέγει η εκάστοτε υπηρεσία η εφαρμογή είναι οι ελαχιστες απαραίτητες για τη λειτουργία της. Η ENACSO, στοχεύοντας πρωτίστως στην προστασία των ανηλίκων, προτείνει επίσης, τη θέση της ηλικίας των 18 ετών ως όριο για τη συμμετοχή σε οποιαδήποτε υπηρεσία εντοπισμού και την απαίτηση γονικής συναίνεσης για τους ανηλίκους. Οποιοσδήποτε λαμβάνει στοιχεία εντοπισμού ενός ανηλίκου μέσω μιας υπηρεσίας θα πρέπει να λαμβάνει γι' αυτό ad hoc έγκριση, τόσο από τον ανήλικο, όσο και από τον κηδεμόνα τους, παρέχοντας στοιχεία προσωπικής ταυτοποίησης. Επιπλέον, οι εφαρμογές που υλοποιούν τεχνολογίες εντοπισμού θα πρέπει να εξασφαλίσουν στοιχεία εξακρίβωσης της ηλικίας των μελών τους.

Αξίζει να σημειωθεί μια σημαντική πρόβλεψη του δικαίου των ΗΠΑ, που δεν έχει ίσως λάβει ανάλογη προσοχή από την Ευρωπαική Ένωση: Με βάση την Πράξη Προστασίας της Ιδιωτικότητας της Θέσης του 2011 (Location Privacy Protection Act of 2011)[96], αν μια εταιρία συλλέγει και μοιράζεται δεδομένα θέσης με τρίτους, όπως διαφημιστές, και λαμβάνει δεδομένα για πάνω από

94 http://www.enacso.eu/

95 Child protection concerns and the new location services, Submission to the W3C Privacy Workshop on Advanced Web APIs, 12/13 Ιουλίου 2010, Λονδίνο, http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-9.pdf

96 http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.1223:

5.000 συσκευές, τότε οφείλει να λάβει επιπλέον μέτρα για την προστασία των δεδομένων από απειλές, να ενημερώσει άμεσα τους καταναλωτές για την κατοχή των δεδομένων και να τα διαγράψει άμεσα μετά από αίτηση του χρήστη. Η πρόβλεψη αυτή, απευθυνόμενη κατ' ουσία προς τις Apple και Google, έχει σημασία γιατί αναγνωρίζει την ηγεμονική θέση των δύο αυτών εταιριών στην αγορά και αποδίδει σε αυτές μεγαλύτερο βάρος προστασίας και διαχείρισης των δεδομένων που τους έχουν εμπιστευθεί οι χρήστες.

Περαιτέρω ζητήματα

Όπως αναφέρθηκε στην εισαγωγή, ενδιαφέρον για την προστασία της ιδιωτικότητας έναντι της τεχνολογίας υπήρχε ανέκαθεν, αλλά είναι μάλλον πρόσφατη η συνειδητοποίηση ότι η προστασία αυτή διακυβεύεται σε σημαντικό βαθμό από συσκευές και υπηρεσίες που οι περισσότεροι χρησιμοποιούμε καθημερινά, χωρίς να συνειδητοποιούμε πόσες πληροφορίες συγκεντρώνουν για την κίνηση, τις συνήθειες και τις προτιμήσεις μας, σε προσωπικό και επαγγελματικό επίπεδο.

Σήμερα έχουμε πρόσβαση σε πλειάδα υπηρεσιών βασισμένων στην τοποθεσία (location-based services). Στο πλαίσιο αυτών, είναι δυσχερές να γνωρίζουμε τι είδους δεδομένα θέσης καταγράφονται, από ποιον και με ποιο τρόπο μπορεί να αποφευχθεί η καταγραφή. Ο μέσος άνθρωπος έχει την εύλογη προσδοκία για ένα minimum προστασίας του προσωπικού του χώρου, η οποία όμως, όπως φαίνεται, δεν συμπορεύεται με τις τεχνολογικές εξελίξεις.

Όπως αναφέρει ο Simson Garfinkel στο βιβλίο του "Database Nation:

The Death of Privacy in the 21st Century":

> *"Λίγοι μηχανικοί θα προσπαθούσαν να φτιάξουν συστήματα σχεδιασμένα να συνθλίψουν της ιδιωτικότητα και την αυτονομία, και λίγες επιχειρήσεις ή ιδιώτες θα εφάρμοζαν ή αγόραζαν με τη θέλησή τους τέτοια συστήματα, αν γνώριζαν τις συνέπειες. Αυτό που συμβαίνει συχνόταρα είναι ότι οι επιπτώσεις μια νέας τεχνολογίας στην ιδιωτικότητα περνάνε απαρατήρητες ή ότι κι όταν λαμβάνονται υπόψη, δεν γίνονται κατανοητές. Κι αν ακόμα γίνουν κατανοητές, η εφαρμογή τους γίνεται λανθασμένα. Στην πράξη, ακόμα και ελάχιστα σφάλματα μπορούν να μετατρέψουν ένα σύστημα σχεδιασμένο να προστατέψει προσωπικές πληροφορίες σε κάτι που καταστρέφει τα μυστικά μας".*

Η έρευνα σε μεθόδους, όπως το RDF Geotagging,[97] που επιτρέπει τη δημιουργία δεσμών μεταξύ φωτογραφιών που έχουν αναρτηθεί από διάφορους, μη συνδεδεμένους μεταξύ τους χρήστες, βάσει των γεωγραφικών μεταδεδομένων τους, ώστε να επιτρέπεται η άμεση πλοήγηση μεταξύ τους, καθώς και σε τομείς όπως η αυτόματη αναγνώριση προσώπων και η επισήμανση αυτών σε φωτογραφίες[98], προμηνύουν ότι οι οργουελικοί προβληματισμοί πάνω στα ζητήματα προστασίας της γεωγραφικής ιδιωτικότητας των χρηστών της τεχνολογίας θα αυξηθούν με την πάροδο του χρόνου. Αυτή η γνώμη διαμορφώνεται σε πεποίθηση, αν λάβουμε υπ' όψη και την τάση της μετακίνησης της αποθήκευσης δεδομένων από τα τερματικά συστήματα των χρηστών στους server των παρόχων υπηρεσιών (Cloud

97 Torniai, Battle, and Cayzer (2006)

98 Stone, Zickler, and Darrell (2008)

computing/storage). Αφ' ης στιγμής τα δεδομένα των χρηστών αποθηκεύονται σε υπολογιστικά συστήματα πέραν του ελέγχου τους, η αποκάλυψή της επαφίεται στις δυνατότητες και στις επιλογές τρίτων. Το ζήτημα προφανώς αποκτά μεγαλύτερες διαστάσεις, αν λάβουμε υπ' όψη τη δομή της αγοράς των φορητών συσκευών και εν τέλει το πόσο λίγες είναι οι εταιρίες στις οποίες εκατομμύρια χρήστες έχουν εμπιστευθεί πολύτιμα προσωπικά δεδομένα.

Στην παρούσα φάση, η ανάπτυξη τεχνικών κρυπτογράφησης και προστασίας δεδομένων θέσης, η υλοποίηση εργαλείων που αποδίδουν στους χρήστες μεγαλύτερο έλεγχο στην αποκάλυψη δεδομένων, τόσο εκ των προτέρων, όσο και εκ των υστέρων, η επίγνωση των χρηστών για το πόσα και ποια δεδομένα αποκαλύπτουν με τις ενέργειες τους, και ο εναρμονισμός της νομοθεσίας με τις τεχνολογικές εξελίξεις μπορεί να εξασφαλίσει ένα minimum προστασίας.

Βιβλιογραφία

Andrew E. Fano (1998) 'Shopper's Eye: Using Location-based Filtering for a Shopping Agent in the Physical World', *Autonomous Agents* [online]. Available at: http://www.accenturexperience.com/SiteCollectionDocuments/jp-ja/PDF/technology/emerging-technology/mobile-solutions/Accenture_technology_shopperseyeagents98.pdf.

Baik Hoh and Gruteser, M. (2005) 'Protecting Location Privacy Through Path Confusion', IEEE, pp.194–205.

Bayir, M.A., Demirbas, M. and Eagle, N. (2009) 'Discovering spatiotemporal mobility profiles of cellphone users', IEEE, pp.1–9.

Beresford, A. and Stajano, F. (2003) 'Location privacy in pervasive computing', *IEEE Pervasive Computing*, Vol. 2 No. 1, pp.46–55.

Chris Woodyard (21-12-2009) 'Thieves stealing your GPS can track you back home', *USA Today*.

Feldmann, A., Mathy, L., Balakrishnan, M., Mohomed, I. and Ramasubramanian, V. (2009) 'Where's that phone?', ACM Press, p.294.

Friedland, G. and Sommer, R. (2010) 'Cybercasing the Joint: On the Privacy Implications of Geo-Tagging', *HotSec'10 Proceedings of the 5th USENIX conference on Hot topics in security, 2010*, USENIX Association Berkeley, Berkeley, California, USA.

George Alisson (2006) 'Living online: The end of privacy?', *New Scientist Tech*, September.

Gruteser, M. and Grunwald, D. (2003) 'Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking', ACM Press, pp.31–42.

Gruteser, M. and Liu, X. (2004) 'Protecting privacy in continuous location-tracking applications', *IEEE SECURITY & PRIVACY*.

Guo, C., Liu, Y., Shen, W., Wang, H.J., Yu, Q. and Zhang, Y. (2009) 'Mining the Web and the Internet for Accurate IP Address Geolocations', IEEE, pp.2841–2845.

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999) 'Building consumer trust online', *Communications of the ACM*, Vol. 42 No. 4, pp.80–85.

Huffaker, D. (2006) 'Teen Blogs Exposed: The Private Lives of Teens Made Public', *American Association for the Advancement of Science (AAAS)*.

Jarvinen, J., DeSalas, J. and LaMance, J. (2002) 'Assisted GPS: A Low-Infrastructure Approach'. Available at: http://www.gpsworld.com/gps/assisted-gps-a-low-infrastructure-approach-734.

Kaasinen, E. (2003) 'User needs for location-aware mobile services', *Personal and Ubiquitous Computing*, Vol. 7 No. 1, pp.70–79.

Kate Maternowski (2006) 'Campus police use Facebook'.

Kate Murphy (11-8-2010) 'Web Photos That Reveal Secrets, Like Where You Live', *New York Times*.

Kido, H., Yanagisawa, Y. and Satoh, T. (2005) 'Protection of Location Privacy using Dummies for Location-based Services', IEEE, p.1248.

Krontiris, I., Albers, A. and Rannenberg, K. (2010) 'W3C Geolocation API calls for Better User Privacy Protection'.

Krumm, J. and Horvitz, E. (2004) 'LOCADIO: Inferring Motion and Location from Wi-Fi Signal Strengths', pp.4–13.

Peter Stubley (2006) 'Damilola Taylor: Welcome to modern Britain'. Available at: http://www.courtnewsuk.co.uk/c_famous_crime_cases/a_damilola_taylor/crime_vaults/.

Reid, D.B. (1979) 'An algorithm for Tracking Multiple Targets', *IEEIE TRANSACTIONS ON AUTOMATIC CONTROL*, Vol AC-24 No. 6, pp.843–854.

Security analysis of the Louis protocol for location privacy (2009) 'Aakar, Gupta; Milan, Saini; Anish,Mathuria', IEEE Press Piscataway, NJ, USA ©2009, pp.200–207.

Soliman, S., Agashe, P., Fernandez, I., Vayanos, A., Gaal, P. and Oljaca, M. (2000) 'gpsOne/sup TM/: a hybrid position location system', IEEE, pp.330–335.

Stone, Z., Zickler, T. and Darrell, T. (2008) 'Autotagging Facebook: Social network context improves photo annotation', IEEE, pp.1–8.

Thomas, K., Grie, C. and Nicol, D.M. 'unFriendly - Multi-Party Privacy Risks in Social Netowkring'.

Torniai, C., Battle, S. and Cayzer, S. (2006) 'Sharing, Discovering and Browsing Photo Collections through RDF geo-metadata'.

Weyn, M. and Schrooyen, F. (January 31, 2008) 'A WiFi Assisted GPS Positioning Concept', *Proceeding of the Third European Conference on the Use of Modern Information and Communication Technologies*.

Zhengrong, J. and Jain, R. (June 6, 2008) 'Google enables Location-aware Applications for 3rd Party Developers'. Available at: http://googlemobile.blogspot.com/2008/06/google-enables-location-aware.html.

Zhong, G., Goldberg, I. and Hengartner, U. (2007) 'Louis, Lester and Pierre: Three Protocols for Location Privacy', in Borisov, N. and Golle, P. (Eds.), *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp.62–76.

Zirari, S., Canalda, P. and Spies, F. (2010) 'WiFi GPS based combined positioning algorithm', IEEE, pp.684–688.

Κατάλογος εικόνων

Εικόνα 1: Φωτογραφία ενός ποδηλάτου προς πώληση και απεικόνιση της θέσης του από το Google Street View, βάσει του geotag της φωτογραφίας.....14
Εικόνα 2: Το μήνυμα του Android κατά την ενεργοποίηση του GPS.....20
Εικόνα 3: Οθόνη παρουσίασης των δικαιωμάτων που απαιτεί μια εφαρμογή. Μέσα σε όλα διακρίνεται το δικαίωμα γνώσης της ακριβούς τοποθεσίας.....21
Εικόνα 4: Οι επιλογές ενεργοποίησης ή μη των υπηρεσιών τοποθεσίας ανά εφαρμογή σε μια συσκευή iOS χωρίς GPS ή GSM (iPad 1ης γενιάς).....23
Εικόνα 5: Δημιουργία νέας δημοσίευσης στο Facebook, με δυνατότητα κοινοποίησης της τοποθεσίας.....25
Εικόνα 6: Γραφική αποτύπωση των προκαθορισμένων ρυθμίσεων του Facebook αναφορικά με το εύρος αποκάλυψης προσωπικών στοιχείων. Συγκρίνονται οι ρυθμίσεις των ετών 2005 και 2010.....30
Εικόνα 7: Η φόρμα επιλογής του κύκλου που θα έχει πρόσβαση στις τοπικές πληροφορίες των φωτογραφιών ενός χρήστη.....32
Εικόνα 8: Το interface εισαγωγής νέας ανάρτησης στο Google Plus (μέσω browser υπλογιστή). Φαίνονται τα εικονίδια προσθήκης της θέσης του χρήστη και ο καθορισμός των κύκλων αποδεκτών. της ανάρτησης.....35
Εικόνα 9: Ο αλγόριθμος k-area: Όλες οι ενημερώσεις τοποθεσίας σε μία ζώνη καταγράφονται και δεν αποκαλύπτονται, παρά μόνο αν ο χρήστης περάσει σε άλλη ζώνη. Αν η προηγούμενη ζώνη ήταν από τις προστατευμένες, τότε οι ενημερώσεις τοποθεσίας αυτής της ζώνης αποκρύπτονται, ειδάλλως αποκαλύπτονται. Η διαδικασία επαναλαμβάνεται για κάθε ζώνη που έχει

επισκεφθεί ο χρήστης.....59
Εικόνα 10: Γραφική αναπαράσταση του adaptive-interval cloaking αλγόριθμου. Στο παράδειγμα, υποθέτουμε ότι οι κόμβοι R13, R14, R11, R12, R8, R9, R10 περιέχουν έναν χρήστη. Αν kmin = 5 και ο προστατευμένος χρήστης βρίσκεται στο R11, ο αλγόριθμος χωρίζει τοπεδίο εφαρμογής σε υποπεριοχές, μέχρι τη στιγμή που φτάνει στο R4, που περιέχει λιγότερα από 5 άτομα. Τότε επιστρέφει την περιοχή R1, που είναι η αμέσως προηγούμενη που καλύπτει το kmin.....62
Εικόνα 11: Παράδειγμα διάταξης μιας ζώνης ανάμιξης. Οι θέσεις Α και Β είναι πιο κοντά απ' ότι οι θέση Γ. Χρήστες που εισέρχονται την ίδια στιγμή στη ζώνη ανάμιξης, προερχόμενοι από τη θέση Α και τη θέση Γ, δεν θα διακρίνονται όταν εισέλθουν στη θέση Β.....65
Εικόνα 12: Γραφική παράσταση του αλγόριθμου διαταραχής τροχιών των Gruteser και Hoh. Οι Α και Β κινούνται σε παράλληλες τροχιές, αλλά ο αλγόριθμος τις μεταβάλει σε τροχιές που τέμνονται. ώστε να προκαλέσει τη σκοπούμενη σύγχυση.....68
Εικόνα 13: Γραφική αναπαράσταση των βημάτων επικοινωνίας του πρωτοκόλλου Louis. Η διακεκομμένη γραμμή δείχνει την προεραιτική, δεύτερη φάση.....71
Εικόνα 14: Η πρόταση των Friedland & Sommer για τον ορισμό της ακρίβειας geotagging φωτογραφιών.....73