# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών

*Μεταπτυχιακό Πρόγραμμα Σπουδών*

*Πληροφοριακά & Επικοινωνιακά Συστήματα*


Μεταπτυχιακή Διατριβή

# Ιχνηλάτηση και ιδιωτικότητα στο Διαδίκτυο - Επισκόπηση τεχνικών και νομικών ζητημάτων


Χρήστος Χατζηγεωργίου

Επιβλέπων Καθηγητής

Κωνσταντίνος Λιμνιώτης


Μάιος 2021

Μάιος 2021


# Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Πληροφοριακά & Επικοινωνιακά Συστήματα


## Μεταπτυχιακή Διατριβή

# Ιχνηλάτηση και ιδιωτικότητα στο Διαδίκτυο – Επισκόπηση τεχνικών και νομικών ζητημάτων


Χρήστος Χατζηγεωργίου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης



Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά & Επικοινωνιακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2021

## Περίληψη

Οι χρήστες του διαδικτύου παρακολουθούνται όλο και περισσότερο και τα προφίλ τους δημιουργούνται και εμπλουτίζονται διαρκώς μέσω της συνεχιζόμενης εξόρυξης των δεδομένων τους. Οι εταιρείες χρησιμοποιούν τα προφίλ αυτά για να παρέχουν εξατομικευμένες υπηρεσίες στους πελάτες τους, με στόχο την αύξηση των εσόδων. Συγκεκριμένα, η συμπεριφορική διαφήμιση εκμεταλλεύεται τα προφίλ των χρηστών, μέσα από τα οποία φαίνονται τα ενδιαφέροντα και τα χαρακτηριστικά τους, όπως η ηλικία και το φύλο, και η δραστηριότητα των αγορών τους.

Μπορεί να υποστηριχθεί ότι η προσαρμογή των διαφημίσεων που προκύπτει από το προφίλ είναι επίσης επωφελής για τους χρήστες, οι οποίοι λαμβάνουν χρήσιμες πληροφορίες και σχετικές διαδικτυακές διαφημίσεις σύμφωνα με τα ενδιαφέροντά τους. Ωστόσο, η παρακολούθηση συμπεριφοράς θεωρείται συχνά ως απειλή για τα δικαιώματα και τις ελευθερίες τους, κυρίως επειδή βασίζεται σε μεγάλο βαθμό στα προσωπικά στοιχεία των χρηστών. Μία πιθανή αρνητική συνέπεια είναι μια κοινωνία παρακολούθησης, όπου όλες οι διαδικτυακές ή φυσικές μας δραστηριότητες καταγράφονται και συσχετίζονται.

Η πίεση από τους υπερασπιστές της ιδιωτικής ζωής έχει αποδειχθεί μέχρι στιγμής αρκετά ανεπαρκής. Το νομικό πλαίσιο και οι σχετικοί κανονισμοί έχουν σημαντικό ρόλο να διαδραματίσουν, ώστε να δημιουργηθούν τα αντίστοιχα κίνητρα στις εταιρείες, με σκοπό να υιοθετήσουν λύσεις διατήρησης και προστασίας της ιδιωτικής ζωής. Γενικότερα, το βάρος της επιβολής του διαδικτυακού απορρήτου πρέπει να μεταφερθεί στις επιχειρήσεις. Αυτό θα ωθήσει τις εταιρείες να ενσωματώσουν το απόρρητο στις διάφορες διαδικασίες - σχετικές με την επιλογή των προϊόντων τους - αντί να αποποιούνται των ευθυνών τους για την προστασία της ιδιωτικότητας και το απόρρητο μέσω της απλής υιοθέτησης δυσνόητων μακροσκελών νομικών ειδοποιήσεων.

Η παρούσα διατριβή κάνει μία επισκόπηση των συναφών τεχνολογιών αλλά και του νομικού πλαισίου, προκειμένου να καταγράψει την τρέχουσα κατάσταση και να αποτιμήσει τα δέοντα μελλοντικά βήματα τόσο σε ρυθμιστικό επίπεδο, όσο και σε επίπεδο υλοποίησης αναγκαίων τεχνολογικών λύσεων.

## Summary

Internet users are being increasingly tracked and profiled and their personal data is processed continuously using advanced data mining techniques. Companies use profiling to provide customised, i.e. personalised, services to their customers, with the goal of increasing revenues. In particular, behavioural advertising takes advantage of profiles of users' interests, characteristics, such as age and gender, and purchasing activities.

It can be argued that customisation resulting from profiling is also beneficial to users, who receive useful information and relevant online ads in line with their interests. However, behavioural tracking is often perceived as a threat to their rights and freedoms, mainly because it heavily relies on users' personal information. One possible negative consequence is a surveillance society or Internet, where all our online or physical activities are recorded and correlated.

Pressure from privacy advocates has so far proved to be quite inadequate. Regulations have an important role to play in incentivising companies to adopt privacy-preserving solutions. More broadly, the burden of enforcing online privacy should be shifted to businesses. This will push companies to integrate privacy into their products and processes, instead of disclaiming liability for privacy in long obscure legal notices.

This thesis provides a survey on the relative technologies, as well as on the corresponding legal framework, with the aim to reflect the current status and evaluate the future steps that need to be done, including both the regulatory reforms as well as the appropriate privacy enhancing technologies.

## Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον επιβλέποντα καθηγητή μου Κωνσταντίνο Λιμνιώτη για την καθοδήγηση του και την βοήθεια του κατά τη διάρκεια υλοποίησης της εργασίας.

Επίσης θα ήθελα να ευχαριστήσω την γυναίκα μου Μαρία για την υπομονή και τη στήριξη που μου πρόσφερε καθ’ όλη την διάρκεια των μεταπτυχιακών μου σπουδών και τα παιδιά μου Βασίλη και Σπύρο για τα ευχάριστα διαλείμματα.

# Περιεχόμενα

# Κεφάλαιο 1

# Εισαγωγή

Η πρόοδος στην ψηφιακή ενσύρματη και ασύρματη τεχνολογία προκαλεί μια εκρηκτική αύξηση όπως καταγράφεται στο [86] τόσο του τύπου των μέσων όσο και των συσκευών που μπορούν να χρησιμοποιήσουν οι επαγγελματίες της διαφήμισης, του μάρκετινγκ και της αναγνωρισιμότητας μιας μάρκας για να φτάσουν στους καταναλωτές. Πέρα από τις αλλαγές στο περιβάλλον του καταναλωτικού μάρκετινγκ (B2C-Business to Consumer), ακόμη και το βιομηχανικό μάρκετινγκ (B2B-Business to Business) διέρχεται καταιγιστικές και συχνά ριζικές αλλαγές στην τακτική, τις τεχνικές, τις προκλήσεις και τις ευκαιρίες.

Πράγματι, οι λέξεις κλειδιά της διαφήμισης και του μάρκετινγκ τα τελευταία χρόνια έχουν μετατοπιστεί από τον "αριθμό προβολών" στο "συμμετοχή καταναλωτή", από "αναγνώριση μάρκας" στο " φήμη μάρκας", από "μηνύματα" σε "συνομιλίες" και από "online" σε "ψηφιακό". Η ενσωμάτωση ασύρματων και κινητών εφαρμογών και διεπαφών έχει μεταμορφώσει με τέτοιο τρόπο το περιβάλλον, ώστε θα ήταν αδιανόητος πριν από μερικά χρόνια [87].

Με την τεχνολογική εξέλιξη να παρέχει διαρκώς νέα εργαλεία και δυνατότητες, το υπολογιστικό νέφος (cloud computing) αντιπροσωπεύει μία ακόμη αλλαγή στην ικανότητα των διαφημιστικών εταιρειών να προσεγγίσουν το στοχοθετημένο κοινό τους και για τους καταναλωτές και τις επιχειρήσεις να αλληλοεπιδράσουν με την κοινότητα του μάρκετινγκ.

Η τεχνολογία νέφους αυξάνει την ικανότητα συλλογής και ανάλυσης δεδομένων και τα περισσότερο «ακριβή» δεδομένα (δηλ. προσωπικά αναγνωρίσιμα στοιχεία για τους καταναλωτές) παραμένει αντικείμενο έντονης δημόσιας συζήτησης.

Οι χρήστες του διαδικτύου παρακολουθούνται ολοένα και περισσότερο καθώς τα προφίλ και τα προσωπικά τους δεδομένα χρησιμοποιούνται εκτενώς ως νόμισμα στην ανταλλαγή υπηρεσιών. Είναι σημαντικό αυτή η νέα πραγματικότητα να γίνει καλύτερα κατανοητή από όλα

τα ενδιαφερόμενα μέρη, εάν θέλουμε να υποστηρίξουμε και να σεβαστούμε το δικαίωμα της ιδιωτικής ζωής [88].

Μπορεί να υποστηριχθεί ότι η προσαρμογή των διαφημίσεων που προκύπτει από το προφίλ είναι επίσης επωφελής για τους χρήστες, οι οποίοι λαμβάνουν χρήσιμες πληροφορίες και σχετικές διαδικτυακές διαφημίσεις σύμφωνα με τα ενδιαφέροντά τους [90]. Ωστόσο, η παρακολούθηση συμπεριφοράς θεωρείται συχνά ως απειλή για το απόρρητο και την ιδιωτικότητα, κυρίως επειδή βασίζεται σε μεγάλο βαθμό στα προσωπικά στοιχεία των χρηστών. Μία πιθανή αρνητική συνέπεια είναι μια κοινωνία παρακολούθησης, όπου όλες οι διαδικτυακές ή φυσικές μας δραστηριότητες καταγράφονται και συσχετίζονται.

Μέρος της μελέτης αυτής παρέχει μια τεχνική ματιά στην συμπεριφορική παρακολούθηση. Παρουσιάζει μια ολοκληρωμένη εικόνα, απαντώντας σε ερωτήσεις όπως: Γιατί παρακολουθούνται οι χρήστες; Ποιες τεχνικές χρησιμοποιούνται; Σε ποιο βαθμό παρακολουθούμαστε σήμερα; Ποιες είναι οι τάσεις; Ποιοι είναι οι κίνδυνοι;

Στην αντίπερα όχθη εξετάζει τις προσπάθειες μετριασμού του προβλήματος της παρακολούθησης και προσπαθεί να απαντήσει σε ερωτήσεις όπως: Ποια προστατευτικά μέτρα υπάρχουν; Τι θα μπορούσαν να κάνουν οι ρυθμιστικές αρχές για τη βελτίωση του απορρήτου των χρηστών; Πόσο αποτελεσματικές ήταν αυτές οι προσπάθειες μέχρι σήμερα;

Γενικά, υπάρχουν πολλοί μηχανισμοί παρακολούθησης και διαφορετικών μορφών [75, 76]. Ίσως ο πιο δύσκολος μηχανισμός που μπορεί να αντιμετωπιστεί για την προστασία του απορρήτου των χρηστών ανήκει στο λεγόμενο δακτυλικό αποτύπωμα του χρήστη (device fingerprinting) - δηλαδή, ένα μοναδικό αναγνωριστικό μιας συσκευής, ενός λειτουργικού συστήματος ή της έκδοσης του προγράμματος περιήγησης που μπορεί να διαβαστεί από μια διαδικτυακή υπηρεσία κατά την περιήγηση του χρήστη, επιτρέποντας την παρακολούθηση του όταν επισκέπτεται διάφορους ιστότοπους που ανήκουν σε διαφορετικές οντότητες. Το δακτυλικό αποτύπωμα είχε καθοριστεί αρχικά ως το δακτυλικό αποτύπωμα του προγράμματος περιήγησης στο [10] και στη συνέχεια γενικεύτηκε για να περιγράψει οποιαδήποτε μοναδική παρουσία που αφήνει μια συσκευή με βάση, π.χ., ένα συγκεκριμένο λογισμικό που είναι εγκατεστημένο στη συσκευή ή συγκεκριμένες ρυθμίσεις μιας συσκευής [77]. Η δυσκολία στην αντιμετώπιση των δακτυλικών αποτυπωμάτων εξαρτάται από το γεγονός ότι δεν βασίζονται

στην αποθήκευσή τους στις συσκευές-πελάτες του χρήστη (όπως στην περίπτωση των cookies) και ως εκ τούτου απαιτούνται εξελιγμένα μέσα που βασίζονται σε σχεδιαστικές λύσεις που λαμβάνουν υπόψη την προστασία των δεδομένων για την αντιμετώπιση των σχετικών κινδύνων για το απόρρητο. Ειδικά στις εφαρμογές για κινητά, η συμπεριφορική διαφήμιση μπορεί να ακολουθεί και να αλληλεπιδρά με τον χρήστη και να στοχεύει παντού και οποιαδήποτε στιγμή [78], δηλαδή διαφημίσεις που δεν έχουν εξατομικευτεί μόνο σύμφωνα με τα διαδικτυακά προφίλ των χρηστών, αλλά και τα φυσικά τους προφίλ — π.χ., διαφημίσεις που έχουν προσαρμοστεί στις τοποθεσίες των χρηστών, στις φυσικές ή στις πνευματικές δραστηριότητές τους κ.λπ. [79].

Το μέσο smartphone έχει περισσότερες από 25 εφαρμογές εγκατεστημένες [81], καθεμία από τις οποίες έχει τα δικά της δικαιώματα πρόσβασης στη συσκευή ανάλογα με τα δικαιώματα που έχει χορηγήσει ο χρήστης. Η πλειοψηφία των εφαρμογών αυτών χρησιμοποιούν βιβλιοθήκες τρίτου μέρους οι οποίες πολλές φορές αποκτούν τα ίδια δικαιώματα με τις εφαρμογές που τις ενσωματώνουν. Το πρόβλημα με τις βιβλιοθήκες αυτές είναι ότι πιθανώς να παρακολουθούν τους χρήστες [84, 85]. Περισσότερες από τις μισές διαθέσιμες εφαρμογές στο Google Play περιέχουν βιβλιοθήκες διαφημίσεων που συνδέονται με διαφημιζόμενους τρίτου μέρους [80]. Τι είναι επίσης αρκετά ενδιαφέρον, στο [82] φαίνεται ότι ακόμη και η χρήση τεχνολογιών που ενισχύουν την ιδιωτικοτήτα, όπως είναι οι εφαρμογές που αποκλείουν/εμποδίζουν την προβολή διαφημίσεων (Ad-Blocking apps, π.χ., [83]) ενδέχεται να αντιμετωπίσουν ζητήματα σχετικά με την προστασία του απορρήτου, δεδομένου ότι η συγκεκριμένη έρευνα δείχνει ότι ούτε οι ad-blockers είναι απαλλαγμένοι από τη χρήση βιβλιοθηκών παρακολούθησης τρίτου μέρους και αιτήσεις αδειών πρόσβασης σε κρίσιμους πόρους στις συσκευές των χρηστών. Επιπλέον, όπως έχει ήδη αναλυθεί στο [81], η χρήση δημοφιλών βιβλιοθηκών από διαφορετικές εφαρμογές στην ίδια συσκεύη, θα μπορούσε να χορηγήσει στις βιβλιοθήκες αυτές τα απαραίτητα δικαιώματα, χρησιμοποιώντας συνδυαστικά τις άδειες στους πόρους του συστήματος, ώστε να συγκεντρώσουν ένα πιθανώς μεγάλο αριθμό προσωπικών δεδομένων χωρίς τη σύμφωνη γνώμη του χρήστη.

Η εκ σχεδιασμού παγκόσμια παρουσία του cloud computing μπορεί επίσης να εκθέσει τα ευαίσθητα προσωπικά δεδομένα των καταναλωτών σε σημαντικές απειλές της ιδιωτικότητας και της ασφάλειας. Η ρύθμιση της ιδιωτικής ζωής και της ασφάλειας των καταναλωτών

αποτελεί μια πρόκληση για τις εθνικές ρυθμιστικές αρχές για την προστασία των προσωπικών δεδομένων ανά τον κόσμο, μιας και σχεδιάστηκαν αρχικά με γνώμονα την προστασία των καταναλωτών εντός των εθνικών συνόρων [89]. Στη νομοθεσία για την προστασία των προσωπικών δεδομένων σε εθνικό και ευρωπαϊκό επίπεδο συγκαταλέγεται ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ ή GDPR) της Ευρωπαϊκής Ένωσης που αφορά την προσπάθεια για τη διαμόρφωση ενός ενιαίου νομοθετικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, χωρίς να απαιτείται ειδική προσαρμογή της εθνικής νομοθεσίας .

Πέραν της σπουδαιότητας του περιεχομένου του GDPR, ανάγκη συμμόρφωσης των επιχειρήσεων επιτάσσουν και οι επιπτώσεις της μη συμμόρφωσης.

Η μη συμμόρφωση επιφέρει μεγάλα πρόστιμα σε όσους δεν λαμβάνουν τα απαραίτητα μέτρα, που, κατά περίπτωση παραβάσεων, ανέρχονται έως τα 20.000.000 ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

Ο GDPR, ωστόσο, δεν είναι το μοναδικό νομοθέτημα που θα επηρεάσει την επεξεργασία προσωπικών δεδομένων τα επόμενα χρόνια. Ένας άλλος Κανονισμός, ο Κανονισμός ePrivacy [91], αποτελεί βασικό κομμάτι της μεταρρύθμισης του πλαισίου της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων και θα συνδιαμορφώσει καταλυτικά το ψηφιακό περιβάλλον μαζί με τον GDPR. Ο Κανονισμός ePrivacy αποτελεί είναι ειδικότερος σε σχέση με τον GDPR, συνεπώς θα εξειδικεύσει, θα συμπληρώσει - και σε ορισμένα σημεία θα υπερισχύσει - του GDPR σε ό,τι αφορά δεδομένα ηλεκτρονικών επικοινωνιών που ανταποκρίνονται στον ορισμό των δεδομένων προσωπικού χαρακτήρα. Στο πεδίο εφαρμογής του ePrivacy εντάσσονται ορισμένες δραστηριότητες με εξαιρετικά αυξημένο ενδιαφέρον, όπως η απευθείας εμπορική προώθηση με τη χρήση ηλεκτρονικού ταχυδρομείου, τα cookies και τα σχετικά online εργαλεία (π.χ. web beacons), καθώς και οι υπηρεσίες/εφαρμογές επικοινωνιών.

## 1.1 Σκοπός της διατριβής

Σκοπός λοιπόν της παρούσας μεταπτυχιακής διατριβής είναι η μελέτη των υπαρχουσών και μελλοντικών τάσεων στην παρακολούθηση χρηστών στο Διαδίκτυο, όπως και τα αντίμετρα που

έχουν προκύψει για την αντιμετώπιση αυτής της συνεχιζόμενης και ραγδαία εξελισσόμενης απειλής για την ιδιωτικότητα και το απόρρητο. Μέρος της έρευνας για τα προστατευτικά μέτρα ενάντια σε αυτή την απειλή εξετάζει κατά πόσο τα αντίμετρα αυτά υπήρξαν αποτελεσματικά μέχρι σήμερα και τι μπορεί να γίνει στο μέλλον για την αντιμετώπιση του φαινομένου της αυξανόμενης παρακολούθησης. Πέραν της μελέτης και παρουσίασης των σχετικών τεχνολογιών, εξετάστηκαν προσπάθειες τόσο σε νομοθετικό και ρυθμιστικό επίπεδο, προσπάθειες της κοινότητας των υπερασπιστών της ιδιωτικής ζωής, όπως και διάφορες δράσεις, προγράμματα και ενέργειες αυτορρυθμιστικού χαρακτήρα της βιομηχανίας ψηφιακής διαφήμισης που αποσκοπούν σε υψηλότερο επίπεδο διαφάνειας και ελέγχου επί της διαδικτυακής συμπεριφορικής διαφήμισης.

Στο μεγαλύτερο τμήμα της η παρούσα διατριβή προσπαθεί να περιγράψει και να αναδείξει το πρόβλημα της παρακολούθησης και την αξιολόγηση των προσπαθειών αντιμετώπισης αυτής. Έγινε συλλογή, επεξεργασία και επιλογή της κατάλληλης βιβλιογραφίας για την ανάλυση των τεχνολογιών παρακολούθησης, της υπάρχουσας νομοθεσίας και των αντίστοιχων ρυθμιστικών αρχών όπως και των αυτορρυθμιστικών προσπαθειών της ίδιας της βιομηχανίας ψηφιακής διαφήμισης.

## 1.2 Δομή της διατριβής

Αυτή η μελέτη είναι δομημένη ως εξής: Μετά το εισαγωγικό Κεφάλαιο 1, το οποίο περιγράφει γενικώς το ερευνητικό ζήτημα που άπτεται της παρακολούθησης («ιχνηλάτησης») των χρηστών, το Κεφάλαιο 2 παρουσιάζει τα κίνητρα πίσω από την παρακολούθηση. Στο Κεφάλαιο 3 παρατίθενται οι κύριες τεχνικές παρακολούθησης. Το Κεφάλαιο 4 περιγράφει πώς γίνεται η παρακολούθηση στο Διαδίκτυο σήμερα και εξετάζει το μέλλον της διαδικτυακής παρακολούθησης. Στο Κεφάλαιο 5 συζητούνται οι κίνδυνοι παρακολούθησης και στο Κεφάλαιο 6 παρουσιάζονται διάφορα αντίμετρα. Τέλος, ο επίλογος περιλαμβάνει συμπεράσματα και συστάσεις που επί του παρόντος προτείνονται για τον μετριασμό των επιπτώσεων της παρακολούθησης.

# Κεφάλαιο 2

## 2.1 Γιατί παρακολουθούνται οι χρήστες του Διαδικτύου;

Με την τεχνολογία να μειώνεται σε κόστος και να αυξάνεται το εύρος των υπηρεσιών και η προσβασιμότητα και καθώς η συνεχόμενη υιοθέτηση ευρυζωνικών υπηρεσιών υψηλής και υπερυψηλής ταχύτητας από τους πολίτες και τις επιχειρήσεις, επεκτείνει τις δυνατότητες, τα χαρακτηριστικά και τις λειτουργίες των συσκευών διασύνδεσης, οι επαγγελματίες της διαφήμισης και του μάρκετινγκ είναι όλο και περισσότερο σε θέση να αξιοποιήσουν αυτές τις τεχνολογικές καινοτομίες με διάφορους τρόπους μέσω:

(1) της αφθονίας νέου περιεχομένου (για παράδειγμα μουσική και βίντεο) και του λογισμικού για το διαδίκτυο και εφαρμογών κινητών συσκευών που αυξάνονται με εκθετικό ρυθμό

(2) των «εφαρμογών», οι οποίες γρήγορα γίνονται η προτιμώμενη μέθοδος, όχι μόνο ουσιαστικά για την επισήμανση αγαπημένων τοποθεσιών ιστού και πρόσβαση στο περιεχόμενο, αλλά και στην ανταλλαγή πληροφοριών στα μέσα κοινωνικής δικτύωσης

(3) της επαναχρησιμοποιήσιμης συλλογής δεδομένων - υπάρχει μια σημαντική αύξηση των δεδομένων σε άμεση διαθεσιμότητα, σε κοινή χρήση, υπό δημιουργία και στη συλλογή δεδομένων; και ενώ η δημιουργία εσόδων και το οικονομικό όφελος από την αξιοποίηση των τεχνολογιών, προκαλεί σε κάποιο βαθμό σύγχυση στην αγορά, δεν έχουμε ξαναδεί τόσο ισχυρή ικανότητα καταγραφής δεικτών διαφήμισης, δημογραφικών, γεωγραφικών και «ευαίσθητων» δεδομένων, όπως προσωπικές πληροφορίες και προτιμήσεις των καταναλωτών

(4) της ραγδαίας επεκτασιμότητας της τεχνολογίας - απότομες αυξήσεις σε υπολογιστικές απαιτήσεις ενός διακομιστή και στις απαιτήσεις εύρους ζώνης αντιμετωπίζονται πιο εύκολα. Γενικά, απότομες αλλαγές στις απαιτήσεις μπορεί συχνά να αντιμετωπιστούν σε δευτερόλεπτα κι όχι σε ημέρες ή εβδομάδες

Η συμπεριφορική στόχευση είναι η πρακτική της προσαρμογής διαδικτυακού περιεχομένου, ιδίως διαφημίσεων, σε επισκέπτες με βάση τις αναζητήσεις τους ή το «προφίλ» τους. Η

διαδικασία κατασκευής αυτού του προφίλ χρησιμοποιώντας την εξόρυξη δεδομένων – την μετατροπή δηλαδή των δεδομένων σε γνώση - είναι γνωστή ως διαδικτυακό προφίλ συμπεριφοράς. Τα δεδομένα που συλλέγονται είναι συνήθως ένα αρχείο καταγραφής της δραστηριότητας ιστού του χρήστη και η διαδικασία συλλογής των δεδομένων αυτών ονομάζεται παρακολούθηση συμπεριφοράς.

Η παρακολούθηση κατηγοριοποιείται σε παρακολούθηση πρώτου και τρίτου μέρους (first and third party). Ο χρήστης αποτελεί το «δεύτερο μέρος» (second party) στην διαδικασία αυτής της αλληλεπίδρασης. Στην παρακολούθηση πρώτου μέρους, η παρακολούθηση πραγματοποιείται από τον ιστότοπο ή την εφαρμογή με την οποία ο χρήστης αλληλεπιδρά άμεσα. Στην παρακολούθηση τρίτων, η παρακολούθηση πραγματοποιείται από άλλες οντότητες «τρίτων» και παρακολουθεί τη δραστηριότητα περιήγησης του χρήστη με την πάροδο του χρόνου και σε διαφορετικές ιστοσελίδες. Για παράδειγμα, το Facebook παρακολουθεί ιστότοπους μέσω του κουμπιού "Μου αρέσει" (Like). Κάθε φορά που ένας χρήστης επισκέπτεται έναν ιστότοπο που περιέχει ένα κουμπί «Μου αρέσει» στο Facebook, το Facebook ενημερώνεται για αυτό, ακόμη και αν ο χρήστης δεν κάνει κλικ σε αυτό το κουμπί.

Οι χρήστες παρακολουθούνται διαρκώς και τα προφίλ τους δημιουργούνται και εμπλουτίζονται μέσω της συνεχιζόμενης εξόρυξης των δεδομένων τους. Οι εταιρείες χρησιμοποιούν τα προφίλ αυτά για να παρέχουν εξατομικευμένες υπηρεσίες στους πελάτες τους, με στόχο την αύξηση των εσόδων. Συγκεκριμένα, η συμπεριφορική διαφήμιση εκμεταλλεύεται τα προφίλ των ενδιαφερόντων, των χαρακτηριστικών των χρηστών, όπως την ηλικία και το φύλο, και τη δραστηριότητα των αγορών τους. Οι διαφημιστικές ή εκδοτικές εταιρείες χρησιμοποιούν στοχευμένη προβολή διαφημίσεων που αντικατοπτρίζουν στενά τα ενδιαφέροντα των χρηστών, π.χ. «φιλόζωος».

Υπάρχουν διάφορα κίνητρα πίσω από την παρακολούθηση στο διαδίκτυο. Η παρακολούθηση πρώτου μέρους (first-party tracking) πραγματοποιείται συχνά από τους κατόχους ιστότοπων για την εξατομίκευση της εμπειρίας χρήστη σε όλες τις περιόδους σύνδεσης, όπως η διατήρηση του καλαθιού αγορών και των προτιμήσεων του χρήστη. Η παρακολούθηση πρώτου μέρους χρησιμοποιείται επίσης για τον εντοπισμό πιθανής απάτης και την επιβολή του νόμου. Στην πραγματικότητα, αρκετοί κανονισμοί απαιτούν από ιστότοπους να καταγράφουν τις

δραστηριότητες των χρηστών με σκοπό την πρόληψη της απάτης, την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, την εθνική ασφάλεια και την επιβολή του νόμου [1]. Δύο σημαντικοί λόγοι για την παρακολούθηση τρίτων είναι η δημιουργία προφίλ χρήστη, η οποία χρησιμοποιείται στη στοχευμένη διαφήμιση και η μέτρηση/ανάλυση των διάφορων διαφημιστικών δράσεων. Αυτές οι δύο πτυχές αναφέρονται λεπτομερώς στο υπόλοιπο αυτής της ενότητας.

2.1.1 Προφίλ χρήστη. Σκοπός της στόχευσης συμπεριφοράς είναι η παρακολούθηση των χρηστών με την πάροδο του χρόνου και η δημιουργία προφίλ των ενδιαφερόντων, των χαρακτηριστικών τους, όπως η ηλικία και το φύλο και της δραστηριότητας αγορών τους. Οι διαδικτυακές διαφημίσεις χρησιμοποιούν συμπεριφορική στόχευση για την προβολή διαφημίσεων που αντικατοπτρίζουν τα ενδιαφέροντα των χρηστών. Κατά μια πρώτη προσέγγιση, τα διαδικτυακά διαφημιστικά συστήματα αποτελούνται από τρεις κύριες οντότητες: τον διαφημιζόμενο, τον εκδότη και το δίκτυο διαφημίσεων. Ο διαφημιζόμενος είναι η οντότητα, όπως ένας κατασκευαστής αυτοκινήτων ή ένα ξενοδοχείο, που θέλει να διαφημίσει ένα προϊόν ή μια υπηρεσία. Ο εκδότης είναι η οντότητα, όπως μια διαδικτυακή εταιρεία εφημερίδων, η οποία διαθέτει έναν ή περισσότερους ιστότοπους και είναι πρόθυμος να εμφανίζει διαφημίσεις και να πληρώνεται για αυτές. Τέλος, το δίκτυο διαφημίσεων είναι η οντότητα που συλλέγει διαφημίσεις από τους διαφημιζόμενους και τις τοποθετεί σε ιστότοπους εκδοτών. Εάν ένας χρήστης κάνει κλικ σε μια διαφήμιση (στο μοντέλο «κόστος ανά κλικ»), το δίκτυο διαφημίσεων εισπράττει πληρωμές από τον αντίστοιχο διαφημιζόμενο και καταβάλλει μέρος αυτής στον εκδότη. Υπάρχει, επομένως, ένα ισχυρό κίνητρο για το δίκτυο διαφημίσεων να δημιουργήσει ακριβή και πλήρη προφίλ προκειμένου να μεγιστοποιήσει την «αναλογία κλικ προς αριθμό εμφανίσεων» και κατά συνέπεια τα έσοδα.

Οι ιστότοποι ηλεκτρονικού εμπορίου, στο πλαίσιο του πρώτου μέρους, χρησιμοποιούν επίσης παρακολούθηση συμπεριφοράς και προφίλ για να προτείνουν προϊόντα που ενδέχεται να ενδιαφέρουν τους χρήστες. Για παράδειγμα, η Amazon προτείνει προϊόντα σε διαδικτυακούς χρήστες με βάση τις προηγούμενες συμπεριφορές ατόμων (εξατομικευμένες προτάσεις), σε προηγούμενες συμπεριφορές παρόμοιων χρηστών (κοινωνική πρόταση) και, φυσικά, σε αντικείμενα που αναζητήθηκαν (πρόταση αντικειμένου).

Με την εμφάνιση των έξυπνων τηλεφώνων (smartphones), πολλές εφαρμογές καταγράφουν τις τοποθεσίες και τις κινήσεις των χρηστών. Οι πληροφορίες τοποθεσίας επιτρέπουν πολλές χρήσιμες υπηρεσίες, όπως οδηγίες οδήγησης, πληροφορίες για το πού βρίσκονται οι φίλοι μας ή προτάσεις για κοντινά εστιατόρια. Ωστόσο, αυτές οι πληροφορίες συλλέγονται επίσης από τους εμπόρους για τη βελτίωση του προφίλ. Ενώ τα οφέλη που παρέχονται από αυτά τα συστήματα είναι αδιαμφισβήτητα, δυστυχώς αποτελούν σημαντική απειλή για το απόρρητο της τοποθεσίας, όπως φαίνεται από πολλές έρευνες τόσο για iPhone όσο και για συσκεύες Android [2].

2.1.2 Αναλυτικά στοιχεία / μετρήσεις Ιστού. Η παρακολούθηση χρησιμοποιείται επίσης για διάφορους τύπους συγκεντρωτικών μετρήσεων, όπως στατιστικά στοιχεία επισκεψιμότητας ιστότοπων ή αποτελεσματική έκθεση διαφημίσεων [1]. Αν και είναι τεχνικά εφικτό για τα πρώτα μέρη να πραγματοποιήσουν αυτές τις μετρήσεις από μόνα τους, πολλοί ιστότοποι χρησιμοποιούν εργαλεία ανάλυσης ιστού τρίτων, όπως το Google analytics [3], για τη λήψη συγκεντρωτικών στατιστικών επισκεψιμότητας, όπως σελίδες με τις περισσότερες επισκέψεις ή χώρες προέλευσης των επισκεπτών. Αυτά τα εργαλεία συνήθως παρακολουθούν τους χρήστες για να συλλέγουν τις δραστηριότητες περιήγησής τους και προβάλουν τα στοιχεία αυτά περιοδικά σε συγκεντρωτικά στατιστικά στοιχεία. Αυτά τα στατιστικά στοιχεία χρησιμοποιούνται συχνά από ιστότοπους για τη μέτρηση της αποτελεσματικότητας των διαφημιστικών δράσεων ή για τη βελτιστοποίηση του περιεχομένου τους.

Όπως έχει γίνει ήδη αντιληπτό, η «διαφήμιση» είναι η κινητήριος δύναμη πίσω από την παρακολούθηση των χρηστών του διαδικτύου. Τα διαδικτυακά προφίλ των χρηστών πωλούνται στον υψηλότερο πλειοδότη, χιλιοστά του δευτερολέπτου μετά την έναρξη της επίσκεψής τους σε έναν ιστότοπο [92]. Το Google, το Facebook και άλλες εταιρείες τεχνολογίας διαφημίσεων έχουν μια ακόρεστη επιθυμία για πληροφορίες και όσο περισσότερα γνωρίζουν για τους χρήστες του διαδικτύου, τόσο περισσότερα χρήματα μπορούν να κερδίσουν. Είναι εξαιρετικά επικίνδυνο όμως, πολλές φορές, αυτή η προσπάθεια για τη δημιουργία εσόδων από τα προσωπικά δεδομένα των χρηστών να φτάνει στο σημείο να διαμορφώνει τη συμπεριφορά τους.

# Κεφάλαιο 3

## 3.1 Υπάρχουσες τεχνικές παρακολούθησης

Οι διαδικτυακές τεχνολογίες παρακολούθησης έχουν εξελιχθεί σημαντικά τα τελευταία χρόνια [4, 5]. Σε αυτήν την ενότητα, παρουσιάζονται οι κύριες διαδικτυακές τεχνολογίες παρακολούθησης.

Μία από τις κύριες πηγές πληροφοριών που χρησιμοποιούνται για τη δημιουργία προφίλ προέρχεται από την παρακολούθηση ιστού, δηλαδή την παρακολούθηση χρηστών σε διαφορετικές επισκέψεις ή σε διαφορετικούς ιστότοπους. Τα δεδομένα που συλλέγονται περιλαμβάνουν την ακολουθία των ιστότοπων που επισκέπτονται και των σελίδων που προβλήθηκαν και τον χρόνο που αφιερώνεται σε κάθε σελίδα. Η παρακολούθηση ιστού πραγματοποιείται κυρίως με την παρακολούθηση διευθύνσεων IP και cookies, χρησιμοποιώντας τεχνικές όπως Javascript, supercookies, δακτυλικά αποτυπώματα ή DPI (Deep Packet Inspection). Το τελευταίο χρησιμοποιείται από ορισμένους ISP και αυτή η πρακτική παραμένει αμφιλεγόμενη. Με την εμφάνιση των έξυπνων τηλεφώνων, εξοπλισμένων με όλο και πιο εξελιγμένους αισθητήρες, η τοποθεσία και οι φυσικές δραστηριότητες γίνονται επίσης σημαντικές πηγές πληροφοριών για το προφίλ.

**3.1.1 Cookies**. Ένα cookie είναι ένα κομμάτι κειμένου που αποθηκεύεται από το πρόγραμμα περιήγησης ιστού ενός χρήστη και μεταδίδεται ως μέρος ενός αιτήματος HTTP. Αποτελείται από ένα ή περισσότερα ζεύγη ονόματος-τιμής που περιέχουν bits πληροφοριών και ορίζεται από έναν διακομιστή ιστού. Υπάρχουν δύο τύποι cookies: cookies περιόδου σύνδεσης (session) και μόνιμα cookies (persistent). Τα cookies περιόδου σύνδεσης είναι προσωρινά cookies που χρησιμοποιούνται συχνά για την αποθήκευση επιλογών χρήστη ή της κατάστασης πλοήγησης. Ρυθμίζονται από μια υπηρεσία όταν ένας χρήστης συνδέεται και διαγράφονται όταν ο χρήστης αποσυνδεθεί. Τα μόνιμα cookies χρησιμοποιούνται συχνά για την αποθήκευση αναγνωριστικών πληροφοριών, προτιμήσεων χρήστη ή διακριτικών ελέγχου ταυτότητας για τη διατήρηση μιας ταυτότητας με τον διακομιστή. Αυτά τα αρχεία παραμένουν στο πρόγραμμα περιήγησης του χρήστη μέχρι να διαγραφούν ρητά ή να λήξουν. Αποστέλλονται αμετάβλητα

από το πρόγραμμα περιήγησης του χρήστη κάθε φορά που αποκτά πρόσβαση σε αυτόν τον ιστότοπο κι ως εκ τούτου, μπορούν να χρησιμοποιηθούν από ιστότοπους για την παρακολούθηση των χρηστών στις επισκέψεις. Τα μόνιμα cookies δημιουργούν σοβαρά προβλήματα σχετικά με την παραβίαση του απορρήτου και της ιδιωτικότητας. Αποστέλλονται μόνο στους ιστότοπους που τα όρισαν ή σε διακομιστές στον ίδιο τομέα. Ωστόσο, μια ιστοσελίδα ενδέχεται να περιέχει εικόνες, συνδέσμους, web beacons, HTML IFrame, JavaScript ή άλλα στοιχεία που είναι αποθηκευμένα σε διακομιστές σε άλλους τομείς. Τα cookies που ορίζονται κατά την ανάκτηση αυτών των στοιχείων ονομάζονται cookies τρίτων, σε αντίθεση με τα cookies πρώτου μέρους. Ορισμένοι ιστότοποι, όπως διαφημιστικές εταιρείες, χρησιμοποιούν cookies τρίτων για την παρακολούθηση χρηστών σε πολλούς ιστότοπους. Συγκεκριμένα, μια διαφημιστική εταιρεία μπορεί να παρακολουθεί έναν χρήστη σε όλες τις σελίδες όπου έχει τοποθετήσει διαφημιστικές εικόνες ή web beacons. Η γνώση των σελίδων που επισκέπτεται ένας χρήστης επιτρέπει στη διαφημιστική εταιρεία να στοχεύει διαφημίσεις σύμφωνα με τις υποτιθέμενες προτιμήσεις των χρηστών.

**3.1.2 Javascript**. Πολλοί ιστότοποι περιέχουν εκτελέσιμα αρχεία Javascript που κατεβάζονται από χρήστες που τους επισκέπτονται. Αυτά τα αρχεία ενημερώνουν μερικές φορές τα cookies πρώτου μέρους και στέλνουν πληροφορίες στους διακομιστές. Τα προγράμματα Javascript έχουν περιορισμένη πρόσβαση σε δεδομένα χρήστη. Ωστόσο, μπορούν να έχουν πρόσβαση σε πληροφορίες που είναι αποθηκευμένες στο πρόγραμμα περιήγησης, συμπεριλαμβανομένων των προσωρινά αποθηκευμένων αντικειμένων και του ιστορικού των συνδέσμων που επισκέπτονται οι χρήστες.

Μαζί με τα cookies και τα αποτελέσματα της εκτέλεσης JavaScript, οι ιχνηλάτες έχουν όλες τις συνήθεις πληροφορίες διαθέσιμες σε ένα τυπικό αίτημα HTTP, εκτός εάν ο χρήστης έχει λάβει ρητά μέτρα για να αποκλείσει ορισμένα από αυτά: τη διεύθυνση IP του χρήστη, τη συμβολοσειρά χρήστη-πράκτορα (δηλαδή, πληροφορίες σχετικά με το πρόγραμμα περιήγησης και πιθανώς πρόσθετα), τρέχουσα και προηγούμενη διεύθυνση URL (μέσω κεφαλίδας Referer), προτίμηση γλώσσας (Κεφαλίδα Accept-Language) κ.λπ.

**3.1.3 Supercookies και Evercookies**. Η χρήση cookies παρακολούθησης είναι αρκετά συχνή και υπάρχουν γνωστές τεχνικές για την αποφυγή τους [6]. Επομένως, υπάρχει μια ώθηση στη

βιομηχανία παρακολούθησης του Διαδικτύου για την ανακάλυψη και ανάπτυξη πιο ισχυρών μηχανισμών παρακολούθησης, που συχνά αναφέρονται ως Supercookies [7]. Ένα από τα πιο σημαντικά supercookies είναι το λεγόμενο «Flash cookie», ένας τύπος cookie που διατηρείται από το Adobe Flash plugin για λογαριασμό εφαρμογών Flash που είναι ενσωματωμένες σε ιστοσελίδες [5]. Δεδομένου ότι αυτά τα αρχεία cookie αποθηκεύονται εκτός του ελέγχου του προγράμματος περιήγησης, τα προγράμματα περιήγησης ιστού δεν παρείχαν παραδοσιακά μια διεπαφή για προβολή, διαχείριση και διαγραφή αυτών των cookies. Συγκεκριμένα, οι χρήστες δεν ειδοποιούνται όταν έχουν οριστεί τέτοια cookies και αυτά τα cookies δεν λήγουν ποτέ. Τα Flash cookies μπορούν να παρακολουθούν τους χρήστες με όλους τους τρόπους που κάνουν τα παραδοσιακά HTTP cookies και μπορούν να αποθηκευτούν ή να ανακτηθούν κάθε φορά που ένας χρήστης έχει πρόσβαση σε μια σελίδα που περιέχει μια εφαρμογή Flash. Τα Flash cookies χρησιμοποιούνται εκτενώς από δημοφιλείς ιστότοπους. Συχνά χρησιμοποιούνται για την παράκαμψη των πολιτικών για HTTP cookies και των προτιμήσεων απορρήτου των χρηστών. Για παράδειγμα, διαπιστώθηκε ότι ορισμένοι ιστότοποι χρησιμοποιούν HTTP και Flash cookies που περιέχουν περιττές πληροφορίες [8]. Δεδομένου ότι τα flash cookies δεν λήγουν, οι ιστότοποι ενδέχεται να αναπαράγουν αυτόματα HTTP cookies από τα Flash cookies, εάν αυτά διαγραφούν. Η επιμονή των supercookies μπορεί να βελτιωθεί περαιτέρω [9]. Αυτός ο νέος τύπος cookie, που ονομάζεται evercookie, είναι ένας συνδυασμός διαφόρων μηχανισμών παρακολούθησης, όπου ο καθένας ενισχύει τους άλλους και είναι σε θέση να αναγνωρίσει έναν πελάτη ακόμα και όταν έχουν αφαιρεθεί τα τυπικά cookies και τα Flash cookies.

### 3.1.4 Παθητική παρακολούθηση / Stateless tracking (Browser/Device fingerprinting).

Μια πρόσφατη μελέτη έδειξε ότι τα προγράμματα περιήγησης μπορούν να αναγνωριστούν με υψηλό βαθμό ακρίβειας χωρίς cookies ή άλλες τεχνολογίες παρακολούθησης [10]. Τα προγράμματα περιήγησης στο Web παρέχουν διάφορες πληροφορίες σε ιστότοπους, όπως γραμματοσειρές, ανάλυση οθόνης κ.λπ., που μπορεί να μην είναι ικανά να αναγνωρίσουν από μόνα τους ένα πρόγραμμα περιήγησης, αλλά μπορούν να το κάνουν όταν χρησιμοποιούνται σε συνδυασμό. Η μελέτη δείχνει ότι ένα δακτυλικό αποτύπωμα ενός προγράμματος περιήγησης είναι αρκετά μοναδικό ώστε να μπορεί, κατά μέσο όρο, να εντοπίσει ένα πρόγραμμα περιήγησης μεταξύ ενός συνόλου 290.000 άλλων προγραμμάτων περιήγησης (αυτή είναι μια συντηρητική εκτίμηση της μοναδικότητας). Το δακτυλικό ή ψηφιακό αποτύπωμα

(fingerprinting) του προγράμματος περιήγησης είναι ένα ισχυρό εργαλείο για την παρακολούθηση χρηστών μαζί με διευθύνσεις IP, cookies και supercookies. Αυτός ο τύπος παρακολούθησης, που ονομάζεται stateless ή παθητική παρακολούθηση είναι ιδιαίτερα προβληματικός, καθώς είναι δύσκολο να εντοπιστεί.

Η αποτύπωση των ψηφιακών αποτυπωμάτων μιας συσκευής είναι η συστηματική συλλογή πληροφοριών μιας συγκεκριμένης απομακρυσμένης συσκευής με σκοπό τον εντοπισμό, την εξακρίβωση και, συνεπώς, τη δυνατότητα παρακολούθησης της δραστηριότητας του χρήστη για σκοπούς δημιουργίας προφίλ. Δεδομένου ότι οι άνθρωποι συνήθως τείνουν να μην μοιράζονται τις συσκευές τους, είτε πρόκειται για κινητό τηλέφωνο, tablet ή φορητό υπολογιστή, η μοναδική αναγνώριση μιας συσκευής σημαίνει μοναδική αναγνώριση του ατόμου που το χρησιμοποιεί. Οι οντότητες που χρησιμοποιούν μηχανισμούς αποτύπωσης ψηφιακών αποτυπωμάτων συλλέγουν συστηματικά πληροφορίες για όλα τις συσκευές που είναι συνδεδεμένα με τους διακομιστές τους με σκοπό την μοναδική αναγνώρισή τους, ώστε να παρακολουθούν την περιήγηση του χρήστη προκειμένου να δημιουργήσουν ένα προφίλ.

Σε αντίθεση με ό, τι πιστεύουν ορισμένοι, αυτό το προφίλ δεν περιορίζεται στη συλλογή και ανάλυση των συνηθειών περιήγησης του χρήστη ή στις αναζητήσεις που πραγματοποιούν στους διακομιστές. Οι πιο προηγμένες τεχνικές επιτρέπουν την καταχώριση των κινήσεων που κάνει ο χρήστης σε ολόκληρη την ιστοσελίδα με το ποντίκι του, εξετάζοντας τα μέρη της οθόνης που περνά περισσότερο χρόνο. Από την άλλη πλευρά, η ανάπτυξη λογισμικού για συσκευές, για παράδειγμα JavaScript ή Flash, διευκολύνει την εφαρμογή διαδικασιών για τη συλλογή πολύ συγκεκριμένων πληροφοριών από τη συσκευή του χρήστη, όπως τον τύπο του προγράμματος περιήγησης, ο τύπος και η έκδοση του λειτουργικού συστήματος, η ανάλυση οθόνης, η αρχιτεκτονική του επεξεργαστή, λίστες γραμματοσειρών κειμένου, προσθηκών ή προγραμμάτων που έχουν εγκατασταθεί, διευθύνσεις IP κ.λπ. Ο κατάλληλος συνδυασμός όλων αυτών των πληροφοριών επιτρέπει τη δημιουργία ενός τύπου μοναδικού δακτυλικού αποτυπώματος συσκευής που το αναγνωρίζει με μοναδικό τρόπο και, επομένως, διαφοροποιεί κάθε χρήστη του Διαδικτύου χωρίς αμφιβολία.

Μέσω αυτών των τεχνικών δακτυλικών αποτυπωμάτων, κατά την πρόσβαση σε έναν ιστότοπο, το πρόγραμμα περιήγησης εκτελεί στη συσκευή του χρήστη και χωρίς να το γνωρίζει, μια σειρά

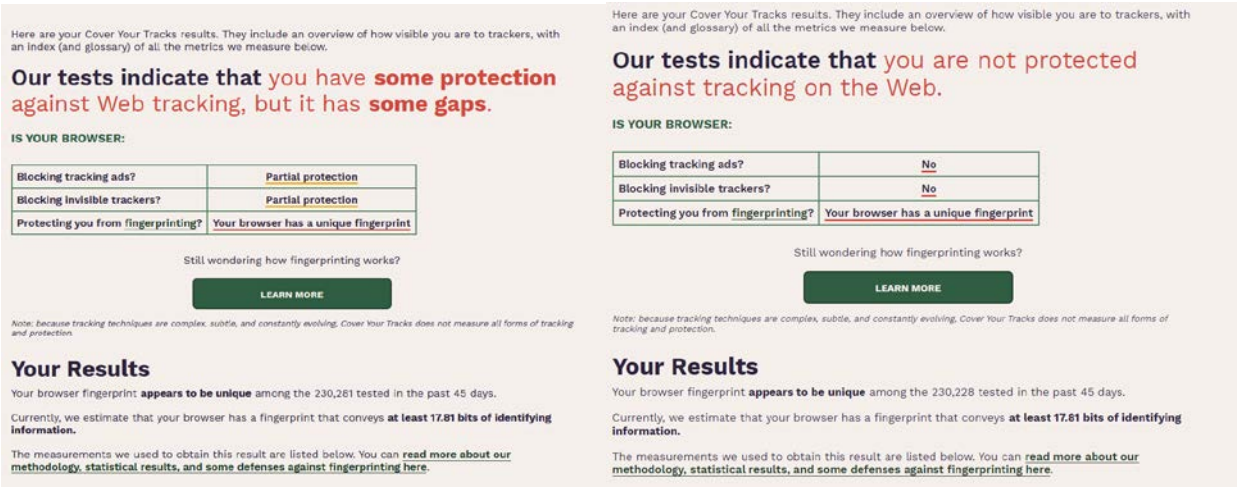
διεργασιών με σκοπό τη συγκέντρωση επαρκώς λεπτομερών πληροφοριών για την μοναδική αναγνώρισή τους και στη συνέχεια τη μεταδίδει στον διακομιστή που τις αποθηκεύει για μεταγενέστερη χρήση. Αυτές οι πληροφορίες συνδυάζονται με άλλα δεδομένα που λαμβάνει ο διακομιστής από το πρόγραμμα περιήγησης του χρήστη, σκοπός των οποίων είναι αρχικά τεχνικός (για παράδειγμα, η προσαρμογή του περιεχομένου στην οθόνη της συσκευής) αλλά τα οποία επαναχρησιμοποιούνται για σκοπούς αναγνώρισης.

Είναι ευρέως γνωστό και αποδεκτό ότι μια συγκεκριμένη υπηρεσία ιστού μπορεί να παρακολουθεί την περιήγηση ενός χρήστη χρησιμοποιώντας cookie, με την εγγύηση ότι η διαγραφή των cookies θα καταργήσει τη σύνδεση μεταξύ της συσκευής και των προσωπικών πληροφοριών που συλλέγονται. Η πραγματικότητα είναι ότι η χρήση των τεχνικών ψηφιακών αποτυπωμάτων της συσκευής επιτρέπει την επανασύνδεση των συνδεδεμένων πληροφοριών στον ίδιο χρήστη κατά τον προσδιορισμό ενός διαγραμμένου cookie, για την αποφυγή της απώλειας της ιχνηλασιμότητας των συνηθειών του προγράμματος περιήγησης του χρήστη. Συμπερασματικά, όταν δημιουργηθεί ένα cookie ταυτότητας, το δακτυλικό αποτύπωμα της συσκευής του ανιχνεύεται και αποθηκεύεται. Όταν ο χρήστης διαγράφει τα cookies στο πρόγραμμα περιήγησής του, αυτά μπορούν να αποκατασταθούν χρησιμοποιώντας το ψηφιακό δακτυλικό αποτύπωμα για να επαναπροσδιορίσουν τον χρήστη, καθιστώντας την διαγραφή των cookies αναποτελεσματική [94].

Υπάρχουν διάφορα ερευνητικά έργα που μας επιτρέπουν να ελέγξουμε εάν ένα πρόγραμμα περιήγησης/συσκευή είναι δυνητικά αναγνωρίσιμο μέσω των διάφορων τεχνικών δακτυλικών αποτυπωμάτων.

Για παράδειγμα ο ιστότοπος PANOPTICLICK [96] πραγματοποιεί μια γρήγορη δοκιμή για να ελέγξει μερικές από τις τεχνικές που αναφέρονται παραπάνω. Το παρακάτω σχήμα δείχνει το αποτέλεσμα μιας δοκιμής που πραγματοποιήθηκε από το PANOPTICLICK, στο πλαίσιο της παρούσας διατριβής, με δύο διαφορετικά προγράμματα περιήγησης. Όπως φαίνεται παρακάτω στη Εικόνα 1 και στα τα δύο προγράμματα περιήγησης τα ψηφιακά αποτυπώματα είναι μοναδικά μεταξύ εκατοντάδων χιλιάδων περιηγητών που ελέγχθηκαν τις τελευταίες 45 ημέρες. Το "bit" είναι μια βασική μονάδα μέτρησης πληροφοριών για υπολογιστές. Το bit αντιπροσωπεύει μια λογική κατάσταση με μία από τις δύο πιθανές τιμές, οι οποίες συχνά

αντιπροσωπεύονται ως "1" ή "0", για παράδειγμα. Στα αποτελέσματά που ελέγχει ο ιστότοπος PANOPTICLICK, ορισμένες μετρήσεις ενδέχεται να αναφέρονται ως "1" ή "0" ή "true" ή "false", υποδεικνύοντας εάν μια ρύθμιση είναι ενεργοποιημένη ή απενεργοποιημένη. Ενώ οι λεπτομέρειες κάθε μεμονωμένης μέτρησης μπορεί να μοιάζουν με μια μικρή ποσότητα πληροφοριών, όταν συνδυάζονται με τις άλλες μετρήσεις του προγράμματος περιήγησής σας, μπορούν να προσδιορίσουν μοναδικά το πρόγραμμα περιήγησής των χρηστών. Τα αποτελέσματά μετρούνται σε "τμήματα αναγνώρισης πληροφοριών", η οποία είναι μια συνδυασμένη περίληψη όλων αυτών των μετρήσεων.




**Εικόνα 1**. Στιγμιότυπα οθόνης αποτελεσμάτων του PANOPTICLICK από δύο ξεχωριστά προγράμματα περιήγησης

Όσον αφορά την υποχρέωση ενημέρωσης των χρηστών, είναι σύνηθες να βρίσκουμε πολιτικές απορρήτου σε ιστότοπους και εφαρμογές που επιτρέπουν στον χρήστη να συναινέσει στη χρήση cookies (αν και σε αρκετές περιπτώσεις δεν υπάρχει ούτε καν αυτή η δυνατότητα), αλλά δεν είναι τόσο συνηθισμένο να βρίσκεις πληροφορίες σχετικά με τη χρήση τεχνικών αποτύπωσης δακτυλικό αποτυπώματος για τη δημιουργία προφίλ.

**3.1.5 Παρακολούθηση τοποθεσίας.** Το API γεωγραφικής θέσης W3C, το οποίο υποστηρίζεται στα προγράμματα περιήγησης Firefox, Opera και Chrome επιτρέπει στους ιστότοπους να ζητούν γεωγραφικές πληροφορίες για τη συσκευή πελάτη. Με την έγκριση του χρήστη, το πρόγραμμα περιήγησης στέλνει πληροφορίες όπως τη διεύθυνση IP του πελάτη, τις διευθύνσεις MAC των συνδεδεμένων σημείων ασύρματης πρόσβασης όπως και τα αναγνωριστικά κυψέλης των δικτύων GSM / CDMA εντός εμβέλειας. Με τη βοήθεια ενός

παρόχου τοποθεσίας δικτύου, όπως οι Υπηρεσίες τοποθεσίας Google, αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για τη λήψη εκτίμησης για την τοποθεσία των συσκευών πελατών. Ενώ το πρόγραμμα περιήγησης στέλνει αυτές τις πληροφορίες μόνο σε έναν ιστότοπο με ρητή έγκριση από τους χρήστες, λίγοι χρήστες αντιλαμβάνονται την ακρίβεια με την οποία αυτές οι υπηρεσίες μπορούν συχνά να εντοπίσουν μια συσκευή. Για παράδειγμα, οι Υπηρεσίες τοποθεσίας Google βασίζονται στις διευθύνσεις MAC των σημείων ασύρματης πρόσβασης που εντοπίστηκαν κατά τη συλλογή δεδομένων του Google Street View για τον εντοπισμό συσκευών πελατών εντός του εύρους ενός ασύρματου σταθμού βάσης IEEE 802.11 (δηλ. κάποιες δεκάδες μέτρα).

# Κεφάλαιο 4

## 4.1 Πώς γίνεται η παρακολούθηση στο Διαδίκτυο;

Στην προηγούμενη ενότητα παρατίθενται ορισμένες από τις υπάρχουσες τεχνικές παρακολούθησης. Σε αυτήν την ενότητα, θα συζητήσουμε πώς αυτές οι τεχνικές χρησιμοποιούνται από εμπόρους, κοινωνικά δίκτυα και εφαρμογές smartphone, για την παρακολούθηση και τη δημιουργία προφίλ των χρηστών.

**4.1.1 Παρακολούθηση τρίτων**. Η αυξανόμενη παρουσία και παρακολούθηση ιστότοπων τρίτων (third-parties) που χρησιμοποιούνται για διαφημίσεις και αναλυτικά στοιχεία έχει αποδειχθεί ήδη σε μια μελέτη πλέον των 10 ετών [11]. Αυτή η μελέτη έδειξε ότι η διείσδυση των κορυφαίων 10 τρίτων μερών αυξήθηκε από 40% το 2005 σε 70% το 2008 και σε πάνω από 70% το Σεπτέμβριο του 2009. Μια άλλη μελέτη δείχνει ότι όχι μόνο αυτά τα τρίτα μέρη αυξάνουν την παρακολούθηση των χρηστών τους, αλλά ότι μπορούν πλέον να συνδέσουν αυτά τα ίχνη με αναγνωριστικά και προσωπικές πληροφορίες μέσω διαδικτυακών κοινωνικών δικτύων [13]. Ωστόσο, πιο πρόσφατα [98] αποδείχθηκε ότι ο συνδυασμός προθέματος UA (User-agent) και IP (ούτε καν πλήρης διεύθυνση) μπορεί να χρησιμοποιηθεί για τον προσδιορισμό ενός κεντρικού υπολογιστή με πιθανότητα 95%. Αυτό υποδηλώνει ότι οι τεχνικές ανωνυμοποίησης που αποθηκεύουν το πρόθεμα IP δεν παρέχουν ιδιωτικότητα.

**4.1.2 Παρακολούθηση διαδικτυακού κοινωνικού δικτύου (OSN)**. Οι πιο δημοφιλείς ιστότοποι κοινωνικής δικτύωσης, όπως το Facebook και το Twitter, παρακολουθούν τους χρήστες σε ολόκληρο τον ιστό. Κάθε ένα από αυτά τα κοινωνικά δίκτυα διαθέτει κοινωνικά γραφικά στοιχεία για κοινή χρήση και προτάσεις (για παράδειγμα κουμπιά "Μου αρέσει", "Tweet" κτλ.) που είναι εγκατεστημένα σε πολλούς ιστότοπους. Αυτά τα κουμπιά επιτρέπουν στα κοινωνικά δίκτυα να παρακολουθούν τους χρήστες, ακόμη και όταν δεν κάνουν κλικ σε αυτά τα κουμπιά - αρκεί να παρακολουθείτε μια ιστοσελίδα με ένα τέτοιο κουμπί.

Σύμφωνα με μελέτες περασμένων ετών, από τους 10K πιο δημοφιλείς ιστότοπους, το 22% περιέχει ένα κουμπί «Like» στο Facebook, το 7,5% ένα κουμπί «Re-Tweet Twitter». Το αξιοσημείωτο από την άποψη της ιδιωτικότητας είναι πως αυτή η μελέτη έδειξε ότι 22 από

τους 77 ιστότοπους σχετίζονταν με την υγεία ή υπηρεσίες υγείας και οι οποίοι περιείχαν ένα κουμπί «Μου αρέσει» στο Facebook. Δεν προκαλεί έκπληξη το γεγονός ότι αυτά τα ποσοστά αυξάνονται χρόνο με το χρόνο [14, 15]. Πρέπει επίσης να σημειωθεί ότι αυτά τα κοινωνικά δίκτυα είναι σε θέση να παρακολουθούν χρήστες που δεν είναι συνδεδεμένοι. Επιπλέον, αυτή η παρακολούθηση είναι δυνατή ακόμη και αν ο χρήστης δεν συμμετέχει στο κοινωνικό δίκτυο, δηλαδή δεν έχει λογαριασμό, εφόσον έχει επισκεφτεί το κοινωνικό δίκτυο τουλάχιστον μία φορά (δηλαδή έχει οριστεί cookie από το κοινωνικό δίκτυο). Στο τελευταίο σενάριο, το κοινωνικό δίκτυο δεν μαθαίνει την ταυτότητα του χρήστη. Ωστόσο, τα αρχεία καταγραφής παρακολούθησης θα μπορούσαν ενδεχομένως να συσχετιστούν με μια ταυτότητα, εάν και όταν ο χρήστης δημιουργήσει λογαριασμό χρησιμοποιώντας το ίδιο πρόγραμμα περιήγησης.

**4.1.3 Παρακολούθηση κινητής συσκευής**. Εκατοντάδες εκατομμύρια άνθρωποι παγκοσμίως χρησιμοποιούν τουλάχιστον ένα smartphone. Αυτά τα κινητά τηλέφωνα έχουν αυξανόμενες υπολογιστικές δυνατότητες και είναι εξοπλισμένα με πολλούς αισθητήρες όπως μικρόφωνα, κάμερες, GPS, επιταχυνσιόμετρα κ.λπ. Περιέχουν επίσης πολλές προσωπικές πληροφορίες για τους ιδιοκτήτες τους: αριθμούς τηλεφώνου, τρέχουσα τοποθεσία, πραγματικό όνομα του ιδιοκτήτη, ένα μοναδικό τηλέφωνο Αριθμό ταυτότητας. Όλο και περισσότερες γεωγραφικές εφαρμογές επιτρέπουν σε άτομα και κοινότητες να συλλέγουν και να μοιράζονται διάφορα είδη δεδομένων.

Οι περισσότεροι χρήστες δεν γνωρίζουν τις επιπλέον πληροφορίες που συλλέγονται για αυτούς πέρα από τα ρητά ζητούμενα δεδομένα. Μια μελέτη της Wall Street Journal [16] έδειξε ότι αρκετές από τις πιο δημοφιλείς εφαρμογές Android ή iPhone, συμπεριλαμβανομένων παιχνιδιών και OSN, διαβίβασε το μοναδικό αναγνωριστικό συσκευής του τηλεφώνου, την τοποθεσία του τηλεφώνου, την ηλικία, το φύλο και άλλα προσωπικά στοιχεία σε εταιρείες τρίτων χωρίς τη συνειδητοποίηση ή τη συναίνεση των χρηστών. Ο κίνδυνος απορρήτου γίνεται υψηλότερος καθώς το όριο μεταξύ OSN και Υπηρεσιών βάσει τοποθεσίας (LBS) γίνεται πιο ασαφές. Για παράδειγμα, OSN όπως το FourSquare και το Facebook έχουν σχεδιαστεί για να ενθαρρύνουν τους χρήστες τους να μοιράζονται τα γεωγραφικά τους δεδομένα, και πληροφορίες που δημοσιεύονται σε κοινωνικές εφαρμογές όπως το Twitter μπορούν να χρησιμοποιηθούν για να συμπεράνουμε αν ένα άτομο βρίσκεται στο σπίτι ή όχι. Άλλες εφαρμογές, όπως το Χάρτες Google (Maps), επιτρέπουν στους χρήστες να παρακολουθούν τις

κινήσεις των κινητών τηλεφώνων των φίλων τους και να εμφανίζουν τη θέση τους σε χάρτη. Εκτός από τις κοινωνικές εφαρμογές, υπάρχουν και άλλες δημόσιες πηγές πληροφοριών που μπορούν να χρησιμοποιηθούν από πιθανούς αντιπάλους, όπως η δωρεάν γεωγραφική γνώση που παρέχεται από τους Χάρτες Google, τους Χάρτες Yahoo! Και το Google Earth.

**4.1.4 Ταυτοποίηση**: Υποστηρίζεται συχνά ότι το μεγαλύτερο μέρος της παρακολούθησης που περιγράφεται παραπάνω είναι ακίνδυνο, επειδή τα ίχνη είναι ανώνυμα. Με άλλα λόγια, παρόλο που οι ιστότοποι είναι σε θέση να παρακολουθούν συσκευές, δεν μπορούν να πουν ποιοι είναι οι χρήστες που βρίσκονται πίσω από αυτούς. Φυσικά, τα πράγματα δεν είναι τόσο απλά στην πράξη. Ένα ίχνος μπορεί συχνά να είναι ανώνυμο και να συνδέεται με μια ταυτότητα μέσω διαφορετικών μεθόδων. Ο Narayanan [17] πρότεινε πρόσφατα μια ταξινόμηση πολλών τρόπων με τους οποίους μπορεί να αναγνωριστεί ένα ψευδώνυμο μέσω του ιστορικού περιήγησης:

1. *Το τρίτο μέρος είναι επίσης πρώτο μέρος*: Το τρίτο μέρος μπορεί να είναι πρώτο μέρος σε άλλο πλαίσιο επεξεργασίας, όπου ο χρήστης παρείχε εθελοντικά την ταυτότητά του. Το Facebook, για παράδειγμα, έχει πάνω από 800 εκατομμύρια χρήστες και επιβάλλει την απαίτηση οι χρήστες να παρέχουν το πραγματικό τους όνομα στην υπηρεσία. Όταν μια σελίδα περιλαμβάνει ένα κοινωνικό widget Facebook τρίτου μέρους, το Facebook προσδιορίζει τον χρήστη για εξατομίκευση του widget.

2. *Ένα πρώτο μέρος πωλεί την ταυτότητα του χρήστη*: Ορισμένοι ιστότοποι πρώτου μέρους παρέχουν σκόπιμα την ταυτότητα ενός χρήστη σε τρίτους, εάν πληρώνονται. Μερικοί έχουν δημιουργήσει ακόμη και ένα επιχειρηματικό μοντέλο, συνήθως εμφανίζονται ως δωρεάν κληρώσεις ή κουίζ. Αρκετοί πάροχοι δεδομένων διαφήμισης αγοράζουν πληροφορίες αναγνώρισης, ανακτούν τον φάκελο του χρήστη από μια βάση δεδομένων καταναλωτών εκτός σύνδεσης και τις χρησιμοποιούν για τη στόχευση διαφημίσεων.

3. *Ένα πρώτο μέρος παρέχει ακούσια την ταυτότητα*: Εάν ένας ιστότοπος τοποθετεί στοιχεία αναγνώρισης σε μια διεύθυνση URL ή έναν τίτλο σελίδας, ενδέχεται να διαρρεύσει ακούσια τις πληροφορίες σε τρίτους. Σε ένα έγγραφο του 2011 [18], οι Krishnamurthy et al. εξέτασε την εγγραφή και την αλληλεπίδραση με 120 δημοφιλείς ιστότοπους για διαρροή πληροφοριών σε

τρίτους. Ανέφεραν ότι ένα σύνολο 48% διέρρευσε ένα αναγνωριστικό χρήστη σε ένα Request-URI ή ένα πρόγραμμα παραπομπής.

4. *Απο-ανωνυμοποίηση*: Το τρίτο μέρος θα μπορούσε να αντιστοιχίσει ψευδώνυμα σε ιστορικά περιήγησης με αναγνωρισμένα σύνολα δεδομένων για να τα αναγνωρίσει ξανά. Η εκ νέου αναγνώριση των διαχρονικών δεδομένων έχει αποδειχθεί σε διάφορα περιβάλλοντα, όπως από τους Narayanan και Shmatikov στο σύνολο δεδομένων του Netflix [19].

Επιπλέον, οι χρήστες συμμετέχουν σε διαφορετικούς ιστότοπους και αφήνουν τμήματα πληροφοριών (διαδικτυακά κοινωνικά αποτυπώματα) για τον εαυτό τους σε πολλά από αυτά. Αυτές οι πληροφορίες είναι συχνά δημόσιες και μπορούν εύκολα να συλλεχθούν για τη δημιουργία προφίλ. Μία πρόκληση εδώ είναι να συγκεντρωθούν όλα τα τμήματα, δηλαδή να συνδεθούν τα διαφορετικά δημόσια ψευδώνυμα στα διαδικτυακά προφίλ ενός χρήστη, δεδομένου ότι οι χρήστες εγγράφονται συνήθως με διαφορετικά ψευδώνυμα σε διαφορετικές υπηρεσίες. Ωστόσο, πρόσφατα αποδείχθηκε ότι ένα σημαντικό μέρος των χρηστών επιλέγει έναν μικρό αριθμό σχετικών και προβλέψιμων ονομάτων χρήστη και τα χρησιμοποιεί σε πολλές υπηρεσίες [20].

Υπάρχει τεράστια εμπορική αξία για τη σύνδεση όλων των διαδικτυακών πληροφοριών σχετικά με ένα άτομο. Ενώ η ακαδημαϊκή μελέτη της σύνδεσης των κοινωνικών προφίλ είναι νέα, οι εμπορικές εταιρείες από καιρό δημιουργούν προφίλ, τα οποία συγκεντρώνουν και τα πωλούν στη «μαύρη αγορά». Οι γνωστοί συγκεντρωτές πληροφοριών που διατίθενται στο κοινό, όπως το Spokeo, χρησιμοποιούν κυρίως δημόσια αρχεία, αλλά τα διαδικτυακά προφίλ γίνονται γρήγορα μέρος του παιχνιδιού [21].

## 4.2 Μελλοντικές τάσεις

Οι τεχνικές παρακολούθησης έχουν εξελιχθεί σημαντικά τα τελευταία χρόνια και θα συνεχίσουν να εξελίσσονται. Στην ενότητα, συζητάμε μερικές από τις μελλοντικές τάσεις παρακολούθησης.

**4.2.1 Πραγματικότητα / Φυσική εξόρυξη**. Η λεγόμενη εξόρυξη πραγματικότητας (Reality mining) βγάζει συμπεράσματα για τις ανθρώπινες σχέσεις και συμπεριφορές από πληροφορίες

που συλλέγονται από smartphone [22]. Αυτές οι πληροφορίες περιλαμβάνουν δεδομένα που συλλέγονται από αισθητήρες κινητών τηλεφώνων, όπως τοποθεσία ή φυσική δραστηριότητα, και δεδομένα που καταγράφονται από τα ίδια τα τηλέφωνα, όπως η διάρκεια των κλήσεων και οι αριθμοί που καλούν. Η εξόρυξη πραγματικότητας θα μπορούσε να βοηθήσει τους χρήστες να προσδιορίσουν πράγματα που πρέπει να κάνουν ή να γνωρίσουν νέα άτομα. Θα μπορούσε επίσης να βοηθήσει στην παρακολούθηση της υγείας. Για παράδειγμα, η παρακολούθηση της κίνησης ενός τηλεφώνου μπορεί να αποκαλύψει αλλαγές στο βάδισμα, οι οποίες θα μπορούσαν να είναι ένας πρώιμος δείκτης παθήσεων ή κατάθλιψης. Η ιδέα της αυτόνομης αναζήτησης είναι ένα πρώτο βήμα προς την εξόρυξη πραγματικότητας. Με την αυτόνομη αναζήτηση, η μηχανή αναζήτησης θα πραγματοποιεί αναζητήσεις για χρήστες χωρίς να χρειάζεται να πληκτρολογήσουν οτιδήποτε με μη αυτόματο τρόπο [23]. Για παράδειγμα, ένας χρήστης μπορεί να περπατάει σε ένα δρόμο και να λαμβάνει εξατομικευμένες πληροφορίες σχετικά με τα μέρη που βρίσκονται κοντά στο κινητό του τηλέφωνο, χωρίς να χρειάζεται να κάνει κλικ σε κανένα κουμπί. Ενώ από τη μία, η υπόσχεση της εξόρυξης πραγματικότητας είναι μεγάλη, από την άλλη, η ιδέα της συλλογής πολυάριθμων προσωπικών πληροφοριών δημιουργεί φυσικά πολλά ερωτήματα σχετικά με την προστασία της ιδιωτικής ζωής και προδίδει τον μελλοντικό κίνδυνο μιας δυστοπικής κοινωνίας παρακολούθησης.

**4.2.2 Επαυξημένης πραγματικότητας**. Σε μια συναρπαστική μελέτη, ο Acquisti και οι συνεργάτες του στο Carnegie Mellon University(CMU) έδειξαν ότι η σύγκλιση της τεχνολογίας αναγνώρισης προσώπων, κοινωνικών δικτύων, εξόρυξης δεδομένων και cloud computing μπορεί να χρησιμοποιηθεί για τη σύνδεση δημόσιων δεδομένων εκτός κι εντός σύνδεσης στο διαδίκτυο, με σκοπό την ανάκτηση πολύ ευαίσθητων πληροφοριών για ένα άτομο [24]. Αρχικά, έδειξαν ότι τα εργαλεία αναγνώρισης προσώπου θα μπορούσαν να χρησιμοποιηθούν για την ταυτοποίηση ανώνυμων διαδικτυακών προφίλ. Ειδικότερα, «τράβηξαν» άγνωστες φωτογραφίες προφίλ από μια δημοφιλή ιστοσελίδα γνωριμιών, όπου οι άνθρωποι χρησιμοποιούν ψευδώνυμα για την προστασία του απορρήτου. Στη συνέχεια, συνέκριναν αυτές τις φωτογραφίες, χρησιμοποιώντας αναγνώριση προσώπου, με φωτογραφίες που είναι διαθέσιμες σε δημόσια προφίλ στο Facebook κι έδειξαν ότι ήταν σε θέση να ταυτοποιήσουν ένα σημαντικό ποσοστό των μελών του ιστότοπου γνωριμιών. Επιπλέον, απέδειξαν ότι είναι δυνατή η απόκτηση της ταυτότητας των ξένων στο δρόμο, χρησιμοποιώντας φωτογραφίες

αγνώστων με web κάμερα και συγκρίνοντάς αυτές με εικόνες από προφίλ Facebook. Μέσω της προσέγγιση αυτής, ταυτοποιήθηκαν περίπου το ένα τρίτο των ατόμων στο πείραμα. Τέλος, αποδείχτηκε ότι είναι δυνατόν να προβλέψουμε τα ενδιαφέροντα και κάποια από τα ψηφία των αριθμών Κοινωνικής Ασφάλισης ορισμένων από τους συμμετέχοντες στο πείραμα, από τη φωτογραφία του προσώπου τους και τις πληροφορίες που ανακτήθηκαν από τους ιστότοπους των κοινωνικών δικτύων τους.

Συμπερασματικά, αυτή η μελέτη υπογραμμίζει σοβαρές ανησυχίες για την προστασία της ιδιωτικής ζωής που προκύπτουν από τη σύγκλιση διαφόρων τεχνολογιών. Με τη βελτίωση της τεχνολογίας εξόρυξης δεδομένων και τη συγκέντρωση όλης της πληροφορίας στο υπολογιστικό νέφος, τέτοιες τεχνικές συμπερασμάτων θα γίνουν όλο και πιο εφικτές. Επιπλέον, δεν είναι σαφές πώς η αυτορρύθμιση, οι μηχανισμοί επιλογής ή ακόμη και νομοθετικές ρυθμίσεις και οι κανονισμοί μπορούν να βοηθήσουν στην αποτροπή αυτού του τύπου αποκάλυψης, καθώς όλα τα αποτελέσματα που παρουσιάστηκαν βασίστηκαν σε διαθέσιμες στο κοινό πληροφορίες.

# Κεφάλαιο 5

## 5.1 Οι κίνδυνοι παρακολούθησης: Ποιοι είναι οι κίνδυνοι παρακολούθησης;

Σε αυτήν την ενότητα αναλύονται συγκεκριμένα παραδείγματα των κινδύνων και των κινδύνων της διαδικτυακής παρακολούθησης.

### 5.1.1 Επιτήρηση (κυβέρνηση, εταιρείες)

Ένας από τους μεγαλύτερους κινδύνους παρακολούθησης είναι η παγκόσμια παρακολούθηση. Αυτή η επιτήρηση μπορεί να πραγματοποιηθεί από την κυβέρνηση, για λόγους ασφαλείας ή πολιτικούς ή από εταιρείες για εμπορικούς λόγους. Όπως περιγράφεται λεπτομερώς σε ένα άρθρο των New York Times [25], οι έμποροι έχουν καταλάβει εδώ και πολύ καιρό τα οφέλη από την καταγραφή και ανάλυση της συμπεριφοράς των χρηστών και με αυτό τον τρόπο, επηρεάζουν τις συνήθειες των καταναλωτών. Ο εντοπισμός σημαντικών αλλαγών στη συμπεριφορά αυξάνει τις πιθανότητες να κάνουν τους πελάτες να στραφούν σε διαφορετικό προϊόν. Αυτή η παρακολούθηση πραγματοποιήθηκε και εξακολουθεί να πραγματοποιείται μέσω διαφορετικών τύπων πιστωτικών και μη καρτών και προγραμμάτων επιβράβευσης των καταναλωτών. Η παρακολούθηση μέσω διαδικτύου είναι ένα πιο ισχυρό εργαλείο, καθώς επιτρέπει στους εμπόρους να προσαρμόσουν τις στρατηγικές τους σχεδόν ακαριαία. Όπως φαίνεται στο [25], οι έμποροι χρησιμοποιούν μοντέλα πρόβλεψης που μπορούν να δείξουν από την αλλαγή συμπεριφοράς ενός χρήστη εάν είναι έγκυος ή διαζευχθεί. Αν και η παρακολούθηση έχει τεράστια οικονομικά οφέλη, εγείρει σοβαρές ανησυχίες για την προστασία της ιδιωτικής ζωής.

Οι εταιρείες προωθούν συχνά το επιχείρημα «τίποτα δεν είναι κρυφό» για να δικαιολογήσουν τις δραστηριότητές τους - γιατί ένας χρήστης να ανησυχεί για το απόρρητό του εάν δεν έχει τίποτα να κρύψει; Ο Daniel J Solove απορρίπτει αυτό το επιχείρημα επισημαίνοντας ότι προέρχεται από μια στενή αντίληψη της ιδιωτικής ζωής ως απόρρητο ή απόκρυψη πληροφοριών [26]. Ο Solove σημειώνει επίσης, ότι οι κίνδυνοι της παραβίασης της ιδιωτικής ζωής δεν εκδηλώνονται απαραίτητα ως ψυχικό τραύμα ή βλάβη. Τα προγράμματα συλλογής

πληροφοριών είναι προβληματικά ακόμη κι αν δεν αποκαλυφθούν πληροφορίες, τις οποίες οι άνθρωποι θέλουν να αποκρύψουν. Οι συλλεγόμενες πληροφορίες μπορεί να είναι λανθασμένες ή παραμορφωμένες και να οδηγήσουν σε λανθασμένες αποφάσεις, οι οποίες μπορεί να δημιουργήσουν απογοήτευση. Οι πιθανές βλάβες είναι λάθος συμπεράσματα, κατάχρηση, έλλειψη διαφάνειας και καταλογισμού ευθυνών.

### 5.1.2 Διακρίσεις υπηρεσιών και διακρίσεις τιμών

Μια άλλη συνέπεια της παρακολούθησης και της δημιουργίας προφίλ είναι η διάκριση ή ο αποκλεισμός από κάποιες υπηρεσίες. Το προφίλ μπορεί να αποκαλύψει ότι ένας χρήστης πάσχει ή έχει την τάση να αναπτύξει μια συγκεκριμένη ασθένεια. Αυτές οι πληροφορίες θα μπορούσαν, για παράδειγμα, να χρησιμοποιηθούν από μια εταιρεία ασφάλισης υγείας για να αρνηθεί την ασφάλιση ή να αυξήσει σημαντικά τα ασφάλιστρα. Η διάκριση των τιμών έχει μακρά ιστορία και αποτελεί κοινή πρακτική σήμερα [27]. Ωστόσο, αυτό συνέβαινε συνήθως μέσω ενός δηλωμένου χαρακτηριστικού του αγοραστή, όπως η ηλικία ή το φύλο του. Με την παρακολούθηση και το προφίλ, οι διακρίσεις στις υπηρεσίες και στις τιμές μπορούν να προσαρμοστούν σε κάθε άτομο. Παραδοσιακά, δεν υπήρχαν ποτέ αρκετά δεδομένα για να γίνει αυτό.

### 5.1.3 Οι κίνδυνοι εξατομίκευσης

Όπως έχει αναφερθεί προηγουμένως, το προφίλ χρησιμοποιείται συχνά από τους παρόχους υπηρεσιών για την εξατομίκευση περιεχομένου στους χρήστες. Ένας ιστότοπος ή μια εφαρμογή ειδήσεων μπορεί να εμφανίζει μόνο ειδήσεις που ταιριάζουν με τα προηγούμενα πρότυπα ανάγνωσης των χρηστών. Ένας ιστότοπος εμπόρου μπορεί να προτείνει μόνο προϊόντα που ταιριάζουν με τα συμπεράσματα, τις ανάγκες ή τις προτιμήσεις του χρήστη. Οι μηχανές αναζήτησης μπορούν να βελτιώσουν τα αποτελέσματα με βάση τα προηγούμενα ερωτήματα και τα κλικ ενός χρήστη. Και φυσικά, οι διαδικτυακές διαφημίσεις στοχεύουν συχνά στη συμπεριφορά του χρήστη. Αυτή η εξατομίκευση προκαλεί ανησυχία. Όπως υποστήριξε ο Eli Pariser, με την εξατομίκευση υπηρεσίας, οι χρήστες παγιδεύονται σε μια «φούσκα φίλτρων» και δεν εκτίθενται σε πληροφορίες που θα μπορούσαν να διευρύνουν τους ορίζοντές του [28]. Σε αυταρχικά κράτη, η εξατομίκευση θα μπορούσε επίσης να χρησιμοποιηθεί για την αύξηση της λογοκρισίας, επιλέγοντας την εμφάνιση ειδήσεων σε συγκεκριμένους χρήστες.

Αντιστρόφως, η εξατομίκευση περιεχομένου και υπηρεσίας μπορεί να αποτελέσει πηγή διαρροής πληροφοριών, καθώς είναι συχνά δυνατό να ανακτηθούν τα ενδιαφέροντα ενός χρήστη από το περιεχόμενο / τις υπηρεσίες που του παρέχονται, χρησιμοποιώντας διάφορες τεχνικές εξόρυξης συμπερασμάτων. Σε έρευνα που διεξήχθη, αποδείχθηκε ότι το ιστορικό google ενός χρήστη μπορεί να ανακατασκευαστεί εν μέρει από τις προτάσεις ερωτημάτων του και ότι το προφίλ ενδιαφερόντων ενός χρήστη μπορεί επίσης να συναχθεί από τις στοχευμένες διαφημίσεις του [29, 30]. Σε ένα συγκεκριμένο παράδειγμα, ένας άντρας ανακάλυψε ότι η έφηβη κόρη του ήταν έγκυος επειδή έλαβε κουπόνια για παιδικές τροφές από το αμερικανικό σούπερ μάρκετ Target. Η έφηβος είχε χαρακτηριστεί ως έγκυος από τη συμπεριφορά των αγορών της [25].

Η δημιουργία προφίλ μέσω εξατομίκευσης περιεχομένου μπορεί να έχει και άλλες συνέπειες. Η πρόσφατη «διάσημη» περίπτωση της Cambridge Analytica κατέδειξε ότι η δημιουργία προφίλ χρηστών μπορεί να οδηγήσει σε χειραγώγησή τους, χωρίς οι ίδιοι να το αντιλαμβάνονται, προκειμένου να στραφούν σε συγκεκριμένες πολιτικές επιλογές. Είναι ένα ιδιαίτερα σημαντικό ζήτημα, αφού σαφώς θέτει σε υψηλή διακινδύνευση ατομικά δικαιώματα και ελευθερίες.

# Κεφάλαιο 6

## 6.1 Προστατευτικά μέτρα. Τι μπορεί να γίνει για τον μετριασμό της παρακολούθησης / δημιουργίας προφίλ;

Όπως φαίνεται σε αυτήν την αναφορά, οι χρήστες παρακολουθούνται συνεχώς και επισημαίνονται κατά τη χρήση του διαδικτύου. Αυτή η ενότητα εξετάζει τα υφιστάμενα τεχνολογικά, νομοθετικά και εκπαιδευτικά μέτρα προστασίας.

### 6.1.1 Τεχνολογικά μέτρα

***Εργαλεία οπτικοποίησης και αποκλεισμού παρακολούθησης***: Υπάρχουν πολλά πρόσθετα των προγραμμάτων περιήγησης, όπως το Lightbeam ή το Privacy Badger, που δείχνουν στους χρήστες πόσα προγράμματα παρακολούθησης ενδέχεται να είναι σε θέση να μάθουν γι'αυτούς. Υπάρχουν επίσης πολλά εργαλεία και πρόσθετα προγραμμάτων περιήγησης που εντοπίζουν και αποκλείουν όλα ή μια λίστα παρακολούθησης τρίτων. Για παράδειγμα, το NoScript είναι ένα πρόσθετο του Firefox που επιτρέπει την εκτέλεση εκτελέσιμου περιεχομένου όπως το JavaScript μόνο εάν φιλοξενείται σε έναν αξιόπιστο τομέα [31].

Η λίστα παρακολούθησης προστασίας (Tracking Protection List - TPL) είναι ένα ακόμη εργαλείο των προγραμμάτων περιήγησης και βασίζεται σε μια λίστα, η οποία καταρτίστηκε από διάφορους οργανισμούς, η οποία περιέχει διευθύνσεις ιστού και ιστότοπων παρακολούθησης με ύποπτη συμπεριφορά. Υπάρχει η δυνατότητα οι χρήστες να προσθέσουν και διευθύνσεις που οι ίδιοι θεωρούν ύποπτες.

Την 1η Ιανουαρίου 2021 η εταιρεία λογισμικού Adobe σταμάτησε να υποστηρίζει και να ενημερώνει τον Flash Player μετά τις επανειλημμένες ανησυχίες σχετικά με την ασφάλεια. Οι μεγάλοι προμηθευτές προγραμμάτων περιήγησης έχουν ήδη απενεργοποιήσει την εκτέλεση του Flash Player μετά την ημερομηνία αυτή. [62]

Επιπλέον, υπάρχουν πολλά εργαλεία ενίσχυσης της ιδιωτικής ζωής που δεν είναι ειδικά για την παρακολούθηση τρίτων, αλλά παρόλα αυτά παρέχουν κάποια προστασία έναντι αυτής.

Παραδείγματα τέτοιων εργαλείων περιλαμβάνουν τις ιδιωτικές λειτουργίες περιήγησης μεγάλων προγραμμάτων περιήγησης [32] ή τα δίκτυα ανωνυμίας [33].

Οι τεχνολογικοί κολοσσοί Apple, Google και Microsoft ανταποκρίνονται στις ανησυχίες περί προστασίας του απορρήτου των χρηστών καθιστώντας πιο δύσκολο για τις εταιρείες να παρακολουθούν τους χρήστες στο διαδίκτυο. Για παράδειγμα, το νέο πρότζεκτ Privacy Sandbox[61] της Google θα απενεργοποιήσει σταδιακά τα cookies παρακολούθησης τρίτων στο Chrome και τη μηχανή περιήγησης Chromium παρέχοντας ταυτόχρονα στους διαφημιζόμενους άλλους τρόπους στόχευσης χρηστών με εξατομικευμένες διαφημίσεις. Βέβαια, παρά τις ανησυχίες σχετικά με την ιδιωτικότητα που πρέπει να λάβουμε υπόψη, οι προτάσεις της Google για το Privacy Sandbox θα έχουν δυνητικά πολύ σημαντικό αντίκτυπο σε εκδότες όπως εφημερίδες και στην αγορά ψηφιακών διαφημίσεων και εγείρουν σοβαρά ερωτηματικά όσον αφορά την αντιμονοπωλιακή νομοθεσία που σχετίζεται με τον κλάδο της τεχνολογίας.

***Εξαίρεση***: Οι περισσότερες εταιρείες παρακολούθησης επιτρέπουν στους χρήστες να ορίσουν cookies εξαίρεσης και ορισμένα εργαλεία όπως το Ninja-cookie[63] κάνουν αυτήν τη διαδικασία απλούστερη. Πολλά διαφημιστικά δίκτυα ερμηνεύουν αυτά τα cookies ως εξαίρεση από τη λήψη στοχευμένων διαφημίσεων, αλλά εξακολουθούν να παρακολουθούν και να σκιαγραφούν το προφίλ του χρήστη. Τα περισσότερα μεγάλα προγράμματα περιήγησης, όπως θα δούμε και παρακάτω στην ενότητα αυτή, εφάρμοσαν μια κεφαλίδα DNT (Do Not Track) που λέει στους ιστότοπους που έχουν επιλέξει οι χρήστες ότι δεν θέλουν να παρακολουθούνται [34], αλλά το World Wide Web Consortium (W3C) κατήργησε την ομάδα εργασίας DNT τον Ιανουάριο του 2019, επικαλούμενη ανεπαρκή υποστήριξη και υιοθέτηση.

Το Do Not Track είναι μια πρόταση τεχνολογίας και πολιτικής που επιτρέπει στους χρήστες να εξαιρεθούν από την παρακολούθηση από ιστότοπους που δεν επισκέπτονται, συμπεριλαμβανομένων υπηρεσιών ανάλυσης, διαφημιστικών δικτύων και κοινωνικών πλατφορμών [34, 1].

Τεχνολογικά, ο μηχανισμός DNT είναι απλός: το πρόγραμμα περιήγησης υποδεικνύει σε ιστότοπους την επιθυμία του χρήστη να εξαιρεθεί από την παρακολούθηση, συγκεκριμένα, μέσω της κεφαλίδας HTTP «DNT: 1». Η κεφαλίδα αποστέλλεται με κάθε αίτημα ιστού (http request) - αυτή περιλαμβάνει τη σελίδα που ο χρήστης επιθυμεί να δει, καθώς και κάθε ένα

από τα αντικείμενα και τα σενάρια που είναι ενσωματωμένα στη σελίδα, συμπεριλαμβανομένων των διαφημίσεων και των ιχνηλατών. Αλλά για να έχει νόημα, οι διαφημιζόμενοι θα πρέπει να σέβονται την προτίμηση των χρηστών να μην παρακολουθούνται. Πώς όμως μπορεί να επιβληθεί αυτό; Υπάρχει ένα φάσμα δυνατοτήτων, που κυμαίνονται από αυτορρύθμιση μέσω της πρωτοβουλίας Network Advertising Initiative, έως εποπτευόμενη αυτορρύθμιση ή «από κοινού ρύθμιση», έως άμεση ρύθμιση. Τουλάχιστον, με την τυποποίηση του μηχανισμού και της έννοιας της εξαίρεσης, η κεφαλίδα DNT υπόσχεται έναν πολύ απλουστευμένο τρόπο για τους χρήστες να εξαιρεθούν σε σύγκριση με τον τρέχοντα μηχανισμό cookies [46]. Τα cookies εξαίρεσης δεν είναι ισχυρά, δεν υποστηρίζονται από όλα τα δίκτυα διαφημίσεων και ερμηνεύονται διαφορετικά από εκείνα που το κάνουν (χωρίς παρακολούθηση έναντι της ερμηνείας χωρίς συμπεριφορική διαφήμιση). Η κεφαλίδα DNT αποφεύγει αυτούς τους περιορισμούς και είναι επίσης ανθεκτική στο μέλλον, καθώς ένα νέο δίκτυο διαφημίσεων δεν απαιτεί καμία ενέργεια από το χρήστη. Το DNT δυστυχώς δεν υιοθετήθηκε ευρέως από τον κλάδο, με τις εταιρείες να αναφέρουν την έλλειψη νομικών εντολών για τη χρήση του, καθώς και ασαφή πρότυπα και οδηγίες για το πώς οι ιστότοποι ερμηνεύουν την κεφαλίδα. Το W3C κατήργησε την ομάδα εργασίας DNT τον Ιανουάριο του 2019, επικαλούμενη ανεπαρκή υποστήριξη και υιοθέτηση. Η Apple διέκοψε την υποστήριξη για το DNT τον αμέσως επόμενο μήνα.

Το 2020, ένας συνασπισμός εταιρειών Διαδικτύου που εδρεύει στις ΗΠΑ ανακοίνωσε την επικεφαλίδα Global Privacy Control [68] που αντικαθιστά πνευματικά την κεφαλίδα Do Not Track. Το GPC εφαρμόζεται αυτήν τη στιγμή σε ολόκληρο τον Ιστό. Ορισμένα προγράμματα περιήγησης, επεκτάσεις και εκδότες υποστηρίζουν ή εφαρμόζουν ήδη το GPC. Οι δημιουργοί ελπίζουν ότι αυτή η νέα κεφαλίδα θα πληροί τον ορισμό των "παγκόσμιων ελέγχων απορρήτου με δυνατότητα χρήστη" που ορίζονται από τη νομοθεσία της Καλιφόρνια και τον Ευρωπαϊκό GDPR. Σε αυτήν την περίπτωση, η νέα κεφαλίδα θα ενισχυθεί αυτόματα από τους υφιστάμενους νόμους και οι εταιρείες θα πρέπει να την τιμήσουν.

***Συστήματα απορρήτου-σχεδιασμού και διατήρησης απορρήτου***: Το απόρρητο ως μέρος της σχεδίασης ενός πληροφοριακού συστήματος συχνά επαινείται ως ουσιαστικό βήμα προς την καλύτερη προστασία της ιδιωτικής ζωής: σε έναν κόσμο όπου η ιδιωτική ζωή κινδυνεύει όλο και περισσότερο από νέες τεχνολογίες πληροφοριών και επικοινωνιών, η αυξανόμενη

άποψη είναι ότι μέρος της θεραπείας πρέπει να προέρχεται από τις ίδιες τις τεχνολογίες. Στο τεχνολογικό μέτωπο, οι τεχνολογίες ενίσχυσης της ιδιωτικής ζωής (Privacy Enhancing Technologies - PETs) αποτελούν ενεργό ερευνητικό θέμα στην επιστήμη των υπολογιστών εδώ και δεκαετίες και έχουν προταθεί διάφορες τεχνικές (συμπεριλαμβανομένων ανωνυμοποιητών, συστημάτων διαχείρισης ταυτότητας, διακομιστών μεσολάβησης, μηχανισμών κρυπτογράφησης, ανώνυμων διαπιστευτηρίων κ.λπ.) . Ωστόσο, η προστασία της ιδιωτικής ζωής από το σχεδιασμό (privacy by design) είναι κάτι περισσότερο από τη χρήση PETs: βασίζεται στην ιδέα ότι οι απαιτήσεις απορρήτου θα πρέπει να λαμβάνονται υπόψη στα πρώτα στάδια του σχεδιασμού ενός συστήματος και μπορεί να έχουν πιθανό αντίκτυπο στη συνολική αρχιτεκτονική του. Έχουν προταθεί μόνο ορισμένες γενικές αρχές απορρήτου, όπως οι αρχές της «Δίκαιης Πρακτικής Πληροφόρησης» το 1974, συμπεριλαμβανομένων των μηχανισμών ειδοποίησης και επιλογής, της ακεραιότητας των δεδομένων και των μηχανισμών επιβολής.

Έχουν προταθεί μερικά συστήματα συμπεριφορικής διαφήμισης, όπως τα Adnostic, PrivAd και RePriv, τα οποία θεωρούν την ιδιωτικότητα ως μία από τις βασικές απαιτήσεις σχεδιασμού. Ο κύριος στόχος αυτών των υλοποιήσεων είναι ο περιορισμός της παρακολούθησης, ενώ εξακολουθεί να υποστηρίζεται η προβολή διαφημίσεων με στόχο τη συμπεριφορά των χρηστών. Το Privad οραματίζεται μια πλήρως τεχνική προσέγγιση για τη μη παρακολούθηση και την ιδιωτική στόχευση [35]. Ο πελάτης δημιουργεί ένα προφίλ χρήστη και, σύμφωνα με αυτό το προφίλ, ζητά σχετικές διαφημίσεις από τον μεσίτη. Ένα αξιόπιστο μέρος, ο «έμπορος», ανωνυμοποιεί τον πελάτη για να αποτρέψει την αναγνώριση του πελάτη από το δίκτυο διαφημίσεων. Η ανωνυμοποίηση βέβαια επηρεάζει την απόδοση και καθιστά την απάτη με κλικ (click fraud) πιο δύσκολο να εντοπιστεί. Στο Adnostic το πρόγραμμα περιήγησης (μέσω ενός πρόσθετου) ενημερώνει συνεχώς ένα προφίλ συμπεριφοράς του χρήστη με βάση τη δραστηριότητα περιήγησης [36]. Το δίκτυο διαφημίσεων προβάλλει διαφημίσεις N (ας πούμε, 10) αντί για 1 και το πρόγραμμα περιήγησης επιλέγει μια από τις 10 με βάση το προφίλ του χρήστη. Τα κλικ σε διαφημίσεις δεν θεωρούνται απόρρητα. Η απαγόρευση παρακολούθησης είναι συμβατική και όχι τεχνική. Το RePriv έχει τον γενικότερο στόχο να επιτρέψει την εξατομίκευση μέσω προφίλ ενδιαφέροντος στο πρόγραμμα περιήγησης [37]. Οι εφαρμογές που μπορεί να έχει είναι εξατομικευμένη αναζήτηση, εξατομίκευση ιστότοπου και στόχευση

διαφημίσεων. Ωστόσο, η στόχευση δεν πραγματοποιείται τοπικά και συνεπάγεται ότι το πρόγραμμα περιήγησης αποστέλλει το προφίλ συμπεριφοράς στον διακομιστή.

Υπάρχει ανάγκη τυποποίησης και συγκέντρωσης των τεχνολογιών βελτίωσης της ιδιωτικής ζωής (PETs), καθώς και για μια ευρέως αποδεκτή μεθοδολογία για την αξιολόγηση τέτοιων τεχνολογιών.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) εργάζεται ενεργά για την ανάπτυξη μιας κοινοτικής πύλης για τη δημοσίευση εργαλείων και των αποτελεσμάτων αξιολόγησής τους από υπηρεσίες και συνεργάτες [64].

### 6.1.2 Ρυθμιστικές και νομοθετικές προσεγγίσεις: Τι έχει γίνει στην ΕΕ / ΗΠΑ / αλλού;

#### 6.1.2.1 Ευρωπαϊκή Ένωση - Γενικός κανονισμός για την προστασία δεδομένων και ePrivacy

Η οδηγία ePrivacy του 2002, 2002/58/ΕΚ (γνωστή και ως Οδηγία e-Privacy), έδωσε εντολή ότι οι ιστότοποι πρέπει να παρέχουν πληροφορίες σχετικά με τις πρακτικές συλλογής δεδομένων τους και πρέπει να επιτρέπουν στους χρήστες να επιλέγουν να μην αποθηκεύουν πληροφορίες στο πρόγραμμα περιήγησής τους, εκτός εάν είναι «απολύτως απαραίτητο» για την παροχή υπηρεσίας και «ζητείται ρητά» από τον χρήστη. Στην πράξη, η οδηγία είχε μικρή ισχύ. Τα κράτη μέλη της Ευρωπαϊκής Ένωσης δεν φαίνεται ότι έλαβαν επαρκή μέτρα για την επιβολή της συμμόρφωσης και, σε πολλές περιπτώσεις, αντιμετώπισαν τις ρυθμίσεις cookies του προγράμματος περιήγησης ως επαρκή εφαρμογή [38].

Μια τροποποίηση του 2009 στην οδηγία ePrivacy, 2009/136/ΕΚ, αντικατέστησε τον κανόνα εξαίρεσης με έναν κανόνα ενεργής συγκατάθεσης [39]. Η ερμηνεία της εν λόγω απαίτησης στα Κράτη-Μέλη δεν είναι απόλυτα ενιαία. . Ορισμένα κράτη πρότειναν ότι οι υπάρχουσες ρυθμίσεις του προγράμματος περιήγησης θα παραμείνουν επαρκείς, και ότι η χρήση τους αποτελεί «σιωπηρή συγκατάθεση».

Τα τελευταία έτη είναι υπό διαμόρφωση νέο νομοθέτημα στην Ευρωπαϊκή Ένωση, το οποίο επίκειται να αντικαταστήσει την Οδηγία e-Privacy: θα πρόκειται για Κανονισμό (e-Privacy Κανονισμός), ο οποίος θα έχει άμεση καθολική ισχύ σε όλα τα Κράτη-Μέλη, αποτρέποντας έτσι «ανομοιογένειες» στην εφαρμογή του. Η τελευταία πρόταση του κανονισμού αυτού, είναι να

απαιτείται ρητή, θετική συναίνεση για κάθε ιστότοπο [40]. Οι αρχές της ΕΕ και των κρατών δυσκολεύονται στην οριστικοποίηση του νέου αυτού νομικού πλαισίου, αφού οι διαβουλεύσεις έχουν αρχίσει εδώ και τέσσερα (4) έτη και συνεχίζονται μέχρι σήμερα (όπως περιγράφεται στη συνέχεια).

#### 6.1.2.2 Γενικός κανονισμός για την προστασία δεδομένων (General Data Protection Regulation - GDPR)

Κομβικό σημείο αποτελεί ο Γενικός Κανονισμός για την προστασία δεδομένων (General Data Protection Regulation - GDPR). Ο Κανονισμός (ΕΕ) 2016/679 [65] για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών αποτελεί ένα ουσιαστικό βήμα για την ενίσχυση των θεμελιωδών δικαιωμάτων των προσώπων στην ψηφιακή εποχή. Επίσης διευκολύνει την επιχειρηματική δραστηριότητα με τη διευκρίνιση των κανόνων για τις επιχειρήσεις και τους δημόσιους φορείς στην ενιαία ψηφιακή αγορά. Με την ενιαία νομοθετική ρύθμιση θα αντιμετωπιστεί επίσης ο σημερινός κατακερματισμός στα διάφορα εθνικά συστήματα και ο περιττός διοικητικός φόρτος.

Ο Κανονισμός τέθηκε σε ισχύ στις 24 Μαΐου 2016 [66] και εφαρμόζεται από τις 25 Μαΐου 2018. Ο Γενικός Κανονισμός για την προστασία δεδομένων (ΓΚΠΔ) διαφυλάσσει και αναπτύσσει τις βασικές αρχές και τα δικαιώματα του υποκειμένου των δεδομένων που προβλέπονται στην προϊσχύσασα Οδηγία 95/46/ΕΚ. Επιπλέον, θεσπίζει νέες υποχρεώσεις για τους οργανισμούς, οι οποίοι οφείλουν να εφαρμόζουν προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, να διορίζουν υπεύθυνο προστασίας δεδομένων σε ορισμένες περιπτώσεις, να σέβονται το νέο δικαίωμα φορητότητας των δεδομένων και να σέβονται την αρχή της λογοδοσίας. Οι ιδιαίτερες συνθήκες που έχουν δημιουργηθεί από την έκρηξη των τεχνολογικών δυνατοτήτων οδήγησαν στην θέσπιση ενός ισχυρού νομικού Ευρωπαϊκού πλαισίου προστασίας, αφού η Οδηγία 95/46/ΕΚ, μετά από περίπου μια εικοσαετία, θεωρείται ότι δεν ανταποκρίνεται πλέον στις ανάγκες της εποχής.

Ο κανονισμός αυξάνει σημαντικά τις υποχρεώσεις τόσο των δημόσιων αρχών όσο και των ιδιωτικών εταιρειών/ οργανισμών/ επιχειρήσεων εντός και εκτός Ευρωπαϊκής Ένωσης.

Σε περίπτωση παράβασης προβλέπονται αυξημένα πρόστιμα, που ανάλογα με το είδος και το μέγεθός της, φτάνουν έως τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών, όταν αφορά σε πολυεθνικές εταιρείες.

Βάσει του δικαίου της ΕΕ, οι Κανονισμοί ισχύουν άμεσα και δεν απαιτούνται μέτρα μεταφοράς τους στην εθνική έννομη τάξη. Επομένως, ο ΓΚΠΔ προβλέπει ενιαίο σύνολο κανόνων περί προστασίας δεδομένων σε ολόκληρη την ΕΕ. Με τον τρόπο αυτόν δημιουργούνται συνεκτικοί κανόνες περί προστασίας δεδομένων σε ολόκληρη την ΕΕ, θεσπίζοντας ένα περιβάλλον ασφάλειας δικαίου από το οποίο μπορούν να επωφεληθούν οι οικονομικοί φορείς και τα φυσικά πρόσωπα ως «υποκείμενα των δεδομένων».

**Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα**

**Αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας:** Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.

**Αρχή του περιορισμού του σκοπού:** Τα δεδομένα προσωπικού χαρακτήρα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 του ΓΚΠΔ.

**Αρχή της ελαχιστοποίησης:** Τα δεδομένα προσωπικού χαρακτήρα είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

**Αρχή της ακρίβειας:** Τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και, όταν είναι αναγκαίο, να υποβάλλονται σε επικαιροποίηση. Πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

**Αρχή του περιορισμού της περιόδου αποθήκευσης:** Τα δεδομένα προσωπικού χαρακτήρα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων

μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

**Αρχή της ακεραιότητας και εμπιστευτικότητας:** Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

**Αρχή της λογοδοσίας:** Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις πιο πάνω Αρχές.

Οι βασικές αρχές και κανόνες του νέου Κανονισμού, υπήρχαν ήδη, όπως για παράδειγμα: νομιμότητα, διαφάνεια, περιορισμός του σκοπού, ασφάλεια των δεδομένων, περιορισμός της περιόδου αποθήκευσης, ακεραιότητα και εμπιστευτικότητα. Αυτό που αλλάζει είναι η εισαγωγή της Αρχής της Λογοδοσίας, δηλαδή της υποχρέωσης των οργανισμών να λογοδοτούν σε κάθε στάδιο της εφαρμογής του Κανονισμού.

#### 6.1.2.3 Κανονισμός ePrivacy (υπό έγκριση)

Η έκδοση του Κανονισμού ePrivacy αποτέλεσε επιτακτική ανάγκη μετά το σκάνδαλο Facebook-Cambridge Analytica [93]. Στην προσπάθειά τους να υποστηρίξουν τον ePrivacy Κανονισμό, ορισμένοι ευρωβουλευτές εξέφρασαν ακόμη και την ανησυχία τους ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ (GDPR) δεν θα ήταν αρκετός για να αποτρέψει την “κακή” χρήση των προσωπικών δεδομένων. Έτσι, παρά την αργή πρόοδο, λόγω κυρίως των ανησυχιών για πιθανές ασυνέπειες στην εφαρμογή των δύο νόμων, η συζήτηση για τον ePrivacy αναζωπυρώθηκε τα τελευταία 2 χρόνια. Το αρχικό εγκεκριμένο σχέδιο του Κανονισμού

ePrivacy του 2017, μόλις πρόσφατα τροποποιήθηκε και βρίσκεται στην τελική ευθεία για την ψήφισή του με την έναρξη του τριμερούς διαλόγου μεταξύ του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής [91]. Ο Κανονισμός αυτός όταν οριστικοποιηθεί και ψηφιστεί, θα καταργήσει την υπάρχουσα Ευρωπαϊκή Οδηγία 2002/58/ΕΚ (e-Privacy Directive - συχνά αναφέρεται άτυπα και ως cookies Directive) και αναμένεται να δώσει στους χρήστες του διαδικτύου επιπλέον προστασία της ιδιωτικής ζωής και έρχεται να επεκτείνει, να συμπληρώσει και να εξειδικεύσει τον Κανονισμό GDPR.

Ο Κανονισμός ePrivacy προσπαθεί να δημιουργήσει ένα ολοκληρωμένο σύνολο κανόνων για τις ηλεκτρονικές επικοινωνίες και θα προστατεύσει το απόρρητο των τελικών χρηστών, την εμπιστευτικότητα των επικοινωνιών τους και την ακεραιότητα των συσκευών τους. Σε αντίθεση με το GDPR, καλύπτει όχι μόνο τα προσωπικά δεδομένα, αλλά και τις απαιτήσεις μέτα-δεδομένων (metadata) και εμπιστευτικότητας και θα ισχύει για εφαρμογές άμεσων μηνυμάτων, τις πλατφόρμες Voice-over-Internet-Protocol (VoIP) και στην επικοινωνία μεταξύ συσκευών.

Πιο ειδικά, όσον αφορά τη χρήση cookies και άλλων τεχνολογιών που περιλαμβάνουν την αποθήκευση πληροφοριών ή τη συλλογή πληροφοριών από τη συσκευή ενός χρήστη, η θέση του Ευρωπαϊκού Συμβουλίου προβλέπει ότι η χρήση αυτών των τεχνολογιών επιτρέπεται μόνο εάν ο χρήστης έχει δώσει συγκεκριμένη, σαφή και ειδική, συγκατάθεση σύμφωνα με το GDPR, ή για συγκεκριμένους σκοπούς που ορίζονται στον κανονισμό ePrivacy. Μια άλλη βασική αρχή είναι ότι οι χρήστες πρέπει να έχουν μια πραγματική επιλογή όσον αφορά τη χρήση των cookies ή παρόμοιων τεχνολογιών. Το τρέχον σχέδιο προτείνει στους οργανισμούς να υπενθυμίζουν στους τελικούς χρήστες το δικαίωμά τους να ανακαλούν τη συγκατάθεσή τους σε περιοδικά διαστήματα (τουλάχιστον μία φορά ετησίως). Η θέση του Συμβουλίου επιδοκιμάζει τη χρήση ενός λεγόμενου «τείχους cookies» (cookies-wall), δηλ. να εξαρτάται η πρόσβαση σε έναν ιστότοπο υπό την προυπόθεση της συγκατάθεσης για τη χρήση cookies ως εναλλακτική λύση σε ένα τείχος επί πληρωμή ή τη δημιουργία ενός λογαριασμού σε έναν ιστότοπο, αλλά μόνο εάν ο χρήστης μπορεί να επιλέξει μεταξύ αυτής της προσφοράς και μιας αντίστοιχης προσφοράς από τον ίδιο πάροχο, που δεν συνεπάγεται τη συγκατάθεση για τη χρήση cookies. Η πρακτική αυτή θεωρείται από πολλούς σύμφωνη με το Δίκαιο των καταναλωτών. Η οδηγία της ΕΕ για την προστασία των καταναλωτών του 2019 ορίζει ότι είναι

νόμιμο να ζητείται αποζημίωση σε αντάλλαγμα για την παροχή μιας υπηρεσίας και ότι αυτή η αποζημίωση μπορεί να περιλαμβάνει προσωπικά δεδομένα. Αυτό το βιώνουμε όλοι κάθε φορά που χρησιμοποιούμε μια μηχανή αναζήτησης ή ένα κοινωνικό δίκτυο: η υπηρεσία είναι δωρεάν σε αντάλλαγμα για τη συλλογή προσωπικών δεδομένων. Ωστόσο, από την πλευρά της προστασίας δεδομένων που προκρίνεται η ελεύθερη επιλογή αυτοδιάθεσης της πληροφορίας, κάτι τέτοιο μοιάζει προβληματικό, όπως αναλύεται στη συνέχεια.

Το πρόβλημα δεν είναι η συλλογή δεδομένων, αλλά εάν αυτό γίνεται με διαφάνεια και με τη συγκατάθεση του χρήστη. Κάθε χρήστης πρέπει να είναι ελεύθερος να αποφασίσει ποια αποζημίωση προτίθεται να δώσει σε έναν πάροχο υπηρεσιών σε αντάλλαγμα για την πρόσβαση στην υπηρεσία του: είτε επί πληρωμής, είτε μέσω εγγράφης στην υπηρεσία, είτε με τη συγκατάθεσή του στη χρήση cookies που επιτρέπει στους εκδότες, μέσω διαφημίσεων, να κερδίσουν έσοδα από την παροχή της υπηρεσίας. Η θέση του Συμβουλίου προβλέπει επίσης ότι οι χρήστες θα μπορούν να συναινέσουν στη χρήση ορισμένων τύπων cookies σε έναν ή περισσότερους παρόχους, μέσω της αντίστοιχης λίστας (whitelisting) στις ρυθμίσεις του προγράμματος περιήγησής τους. Θα απλοποιηθεί η διάταξη για τα cookies, η οποία είχε ως αποτέλεσμα την υπερφόρτωση των χρηστών διαδικτύου με αιτήματα συναίνεσης. Ο νέος κανόνας θα είναι πιο φιλικός προς τον χρήστη, καθώς οι ρυθμίσεις του ίδιου του προγράμματος περιήγησης θα παρέχουν έναν εύκολο τρόπο αποδοχής ή άρνησης των cookie παρακολούθησης και άλλων αναγνωριστικών.

Στο ψηφιακό περιβάλλον, είναι πολλές οι περιπτώσεις στις οποίες για να λειτουργήσει μια υπηρεσία απαιτούνται δεδομένα προσωπικού χαρακτήρα, με αποτέλεσμα τα «υποκείμενα των δεδομένων» (όρος που χρησιμοποιείται για τους χρήστες των οποίων τα προσωπικά δεδομένα υφίστανται επεξεργασία) να λαμβάνουν καθημερινά πολλά αιτήματα συγκατάθεσης που πρέπει να απαντηθούν με κλικ και μετατοπίσεις κουμπιών. Αυτό μπορεί να προκαλέσει ένα είδος «κόπωσης από τα κλικ» όταν η συχνότητα εμφάνισής τους είναι υπερβολική και το πραγματικό αποτέλεσμα προειδοποίησης των μηχανισμών συγκατάθεσης μειώνεται. Ως αποτέλεσμα, οι χρήστες σταματούν να διαβάζουν τις ερωτήσεις συγκατάθεσης. Το γεγονός αυτό ενέχει ιδιαίτερο κίνδυνο για χρήστες, καθώς, συνήθως, η συγκατάθεση ζητείται για πράξεις οι οποίες είναι καταρχήν παράνομες χωρίς τη συγκατάθεσή τους. Η πρόταση του Κανονισμού διευκρινίζει επίσης ότι δεν απαιτείται η συγκατάθεση του χρήστη για μη

εμπιστευτικά cookies που βελτιώνουν την εμπειρία του χρήστη στο Διαδίκτυο (όπως για παράδειγμα το cookie που είναι απαραίτητ για να κρατάει το ιστορικό καλαθιού αγορών) ή cookies που χρησιμοποιούνται από έναν ιστότοπο για τον υπολογισμό του αριθμού των επισκεπτών. Στην πιο πρόσφατη δήλωσή του, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) (European Data Protection Board (EDPB)) επέκρινε αυτές τις δύο πτυχές του προτεινόμενου σχεδίου και επανέλαβε τη θέση του ότι, για την καταπολέμηση της συγκατάθεσης από κόπωση, οι «τοίχοι cookies» πρέπει γενικά να απαγορεύονται και ότι οι φιλικές προς το χρήστη επιλογές ρύθμισης του προγράμματος περιήγησης πρέπει να είναι υποχρεωτικές και όχι απλώς να συνιστώνται.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων εισήγαγε για πρώτη φορά κάποια όρια στο πεδίο της συλλογής και επεξεργασίας προσωπικών δεδομένων και έκανε το πρώτο βήμα προς τη κατεύθυνση της προστασίας της ιδιωτικής ζωής, φέρνοντας σαρωτικές αλλαγές στους οργανισμούς. Αναμένεται ότι και ο νέος κανονισμός θα αναγκάσει τον εκσυγχρονισμό των υπηρεσιών και θα φέρει προκλήσεις στη Διοίκηση Οργανισμών Τεχνολογίας. Υπάρχει η προσδοκία ότι το κόστος αλλά και η ταλαιπωρία αυτών των αλλαγών θα ανταμείψει τη κοινωνία με μεγαλύτερη εξασφάλιση του απορρήτου και αύξηση της προστασίας της ιδιωτικότητας του ατόμου.

#### 6.1.2.4 Ηνωμένες Πολιτείες (ΗΠΑ)

Η Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission - FTC) είναι η κορυφαία ομοσπονδιακή ρυθμιστική αρχή για την προστασία των καταναλωτών. Η FTC έχει περιορισμένη γενική νομική ισχύ: Μπορεί να αποτρέψει μόνο «αθέμιτες ή παραπλανητικές» επιχειρηματικές πρακτικές, τις οποίες η επιτροπή έχει ερμηνεύσει σε μεγάλο βαθμό ότι αποτελούν παραβίαση ρητής υπόσχεσης στους καταναλωτές. Η FTC μπορεί να επιβάλει χρηματικές ποινές μόνο έναντι των παραβατών. Στην πράξη, η FTC έχει, ωστόσο, μεγάλο βαθμό εποπτικής δύναμης: οι επιχειρήσεις διστάζουν να υποστούν το κόστος, το βάρος και τις συνέπειες μιας ομοσπονδιακής δράσης επιβολής του νόμου εναντίον τους. Σηματοδοτώντας το αυξημένο ενδιαφέρον της στην περιοχή, η FTC άσκησε δύο ενέργειες επιβολής που σχετίζονται με την παρακολούθηση ιστού τρίτων το 2011 [59, 60].

Οι γενικοί εισαγγελείς έχουν σε μεγάλο βαθμό παράλληλη εξουσία στη ρύθμιση της παρακολούθησης τρίτων. Μέχρι σήμερα, κανένα γραφείο του γενικού εισαγγελέα δεν άσκησε αγωγή κατά της παρακολούθησης. Οι δικηγόροι της πολιτικής τάξης προσπάθησαν να εγείρουν έναν αριθμό ομοσπονδιακών και πολιτειακών αξιώσεων για τις πρακτικές παρακολούθησης ιστού τρίτων. Στις αρχές της αντιδικίας, αρκετές εταιρείες συμφώνησαν σε διακανονισμούς πολλών εκατομμυρίων δολαρίων (π.χ. Quantcast, σχετικά με τη χρήση των Flash cookies [41]). Πιο πρόσφατα, η τάση ήταν οι εταιρείες να έχουν απορρίψει τις υποθέσεις εναντίον τους [42].

Σήμερα, στις ΗΠΑ δεν υπάρχει συνεπής, εθνικός νόμος περί απορρήτου δεδομένων. Αντ' αυτού, οι επιχειρήσεις προσπαθούν να κατανοήσουν μια μίξη διαφορετικών κανονισμών και νόμων που επιβάλλονται από μεμονωμένες πολιτείες [67] και ρυθμιστικούς φορείς που βασίζονται στη βιομηχανία.

Υπάρχουν μόνο ορισμένοι εθνικοί νόμοι που έχουν θεσπιστεί για τη ρύθμιση της χρήσης δεδομένων σε ορισμένες βιομηχανίες και οι οποίοι είναι ήδη θεσπισμένοι προ 20ετίας ή και παλιότερα:

1974 - Ο νόμος περί απορρήτου των ΗΠΑ που περιγράφει τα δικαιώματα και τους περιορισμούς σχετικά με τα δεδομένα που κατέχονται από κυβερνητικές υπηρεσίες των ΗΠΑ.

1996 - Νόμος περί φορητότητας και λογοδοσίας για την ασφάλιση υγείας (HIPAA) που ρυθμίζει την προστασία της ιδιωτικής ζωής και της ασφάλειας στον κλάδο της υγειονομικής περίθαλψης.

1999 - Gramm-Leach-Bliley Act (GLBA) που διέπει τον τρόπο συλλογής και χρήσης των πληροφοριών σχετικά με την ιδιωτική ζωή των καταναλωτών στη χρηματοοικονομική βιομηχανία.

2000 - Ο νόμος για την προστασία της ιδιωτικής ζωής των παιδιών στο Διαδίκτυο (COPPA) έκανε ένα πρώτο βήμα στη ρύθμιση των προσωπικών πληροφοριών που συλλέχθηκαν από ανηλίκους. Ο νόμος απαγορεύει συγκεκριμένα στις διαδικτυακές εταιρείες να ζητούν προσωπικές πληροφορίες από παιδιά ηλικίας 12 ετών και κάτω, εκτός εάν υπάρχει επαληθεύσιμη γονική συγκατάθεση.

Επιπλέον, λόγω του ότι ο Ευρωπαϊκός Γενικός κανονισμός για την προστασία δεδομένων (GDPR) θεσπίστηκε πρώτος, πολλές αμερικανικές και πολυεθνικές εταιρείες έχουν ήδη καταβάλει προσπάθειες για να επιτύχουν τη συμμόρφωση με το GDPR για να συνεχίσουν να συνεργάζονται με τους ευρωπαίους πελάτες τους. Άλλωστε, ο ίδιος ο GDPR αναφέρει ότι έχει εφαρμογή και σε οργανισμούς εκτός ΕΕ, εφόσουν αυτοί παρέχουν υπηρεσίες της Κοινωνίας της Πληροφορίας εντός ΕΕ. Προκειμένου να αποφευχθεί η περαιτέρω επιβάρυνση της συμμόρφωσης, η νομοθεσία περί απορρήτου δεδομένων των ΗΠΑ θα πρέπει να προσπαθήσει να παραμείνει κοντά στο πρότυπο που έχει ήδη ορίσει ο GDPR.

#### 6.1.2.5 Αυτορρύθμιση της διαδικτυακής διαφήμισης

Η βιομηχανία διαδικτυακής διαφήμισης έχει εναρμονίσει σε μεγάλο βαθμό τις αυτορρυθμιστικές προσπάθειες στις ΗΠΑ (Network Advertising Initiative,NAI και Digital Advertising Alliance, DAA) και την ΕΕ (το Interactive Advertising Bureau Europe, IAB Europe). Και τα τρία προγράμματα επιβάλλουν τις ίδιες βασικές απαιτήσεις σε εταιρείες συμπεριφορικής διαφήμισης [43, 44]:

1. Πρέπει να παρέχουν στους χρήστες πληροφορίες σχετικά με τις πρακτικές συμπεριφορικής διαφήμισης που εκτελούν.

2. Πρέπει να επιτρέπουν στους χρήστες να εξαιρεθούν από τη χρήση δεδομένων για σκοπούς συμπεριφορικής διαφήμισης. Σημειώστε ότι αυτή είναι μια επιλογή για μια συγκεκριμένη χρήση δεδομένων. Η συλλογή και άλλες χρήσεις δεδομένων παρακολούθησης τρίτων δεν επηρεάζονται.

Η συμμετοχή των εταιρειών στην αυτορρύθμιση κυμάνθηκε ανάλογα με τις προσπάθειες των ρυθμιστικών αρχών [45]. Προς το παρόν συμμετέχουν οι περισσότερες από τις μεγαλύτερες εταιρείες διαδικτυακής διαφήμισης και ανάλυσης και οι περισσότερες από τις μικρότερες δεν συμμετέχουν. Τα κοινωνικά δίκτυα και οι πάροχοι περιεχομένου απουσιάζουν σχεδόν εντελώς. Η Digital Advertising Alliance έχει επεκτείνει το πρόγραμμά της σε όλα τα τρίτα μέρη και έχει διευρύνει την απαίτηση επιλογής των καταναλωτών σε σχεδόν όλες τις χρήσεις δεδομένων τρίτων για εξατομίκευση ανά συσκευή (όχι ανά χρήστη) [44].

Οι ερευνητές και οι οργανώσεις της κοινωνίας των πολιτών επικρίνουν σε μεγάλο βαθμό τις προσπάθειες αυτορρύθμισης για το ότι δεν παρέχουν επιλογή έναντι της συλλογής δεδομένων και δεν επιβάλλουν ουσιαστικές ποινές σε εταιρείες που παραβιάζουν την αυτορρύθμιση.

### 6.1.3 Εκπαιδευτική προσέγγιση

Εάν οι καταναλωτές είχαν καλύτερη εκπαίδευση για τη συχνότητα και τις συνέπειες της διαδικτυακής παρακολούθησης, θα μπορούσαν να λάβουν πιο ενημερωμένες αποφάσεις σχετικά με τη χρήση διαδικτυακών τεχνολογιών και υπηρεσιών. Όχι μόνο τότε θα προστατεύονταν καλύτερα με εργαλεία αυτοβοήθειας, αλλά αυτό θα ασκούσε και ανταγωνιστική πίεση σε οντότητες στο διαδικτυακό οικοσύστημα παρακολούθησης και θα οδηγούσε σε μια καλύτερη λειτουργία της αγοράς.

Ποιες δυνατότητες υπάρχουν για την εκπαίδευση των καταναλωτών και πόσο αποτελεσματικές μπορεί να είναι;

Μπορούμε να εντοπίσουμε διάφορους τύπους υφιστάμενων προσπαθειών εκπαίδευσης των καταναλωτών στον τομέα της διαδικτυακής παρακολούθησης.

Γενικές συμβουλές σχετικά με το διαδικτυακό απόρρητο και την ευαισθητοποίηση για την ύπαρξη διαδικτυακού οικοσυστήματος παρακολούθησης. Η Ομοσπονδιακή Επιτροπή Εμπορίου των Ηνωμένων Πολιτειών προσφέρει συμβουλές σχετικά με την ασφάλεια κοινωνικής δικτύωσης και την παρακολούθηση μέσω διαδικτύου. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) έχει δημοσιεύσει μια έκθεση σχετικά με τους κινδύνους απορρήτου των cookies [47]. Το Κέντρο Δημοκρατίας και Τεχνολογίας (Center for Democracy and Technology-CDT) έχει δημοσιεύσει έναν οδηγό για τη συμπεριφορική διαφήμιση, συμπεριλαμβανομένης της παρακολούθησης τρίτων και του αντίκτυπου στην ιδιωτική ζωή [69]. Η ευρωπαϊκή πρωτοβουλία για ασφαλέστερο Διαδίκτυο προωθεί την ασφαλέστερη υπεύθυνη χρήση του Διαδικτύου στους νέους και τα παιδιά [71].

Πρωτοβουλίες για την ενημέρωση των καταναλωτών για εργαλεία αυτοάμυνας. Αναρίθμητοι ιστότοποι προτρέπουν τους καταναλωτές να καθαρίζουν περιοδικά τα cookies και παρέχουν οδηγίες για αυτό. Οργανισμοί υπεράσπισης, όπως το Electronic Frontier Foundation (EFF), ερευνούν συχνά τις τεχνολογίες απορρήτου, συμπεριλαμβανομένων των διαδικτυακών παραλείψεων παρακολούθησης[70].

Πληροφορίες σχετικά με τις πρακτικές συλλογής δεδομένων συγκεκριμένων εταιρειών και των προϊόντων τους στο ηλεκτρονικό σύστημα παρακολούθησης. Δεδομένου ότι οι ίδιες οι εταιρείες είναι συχνά αυτές που κάνουν την παρακολούθηση, υπάρχει μια δυσδιάκριτη γραμμή μεταξύ εκπαίδευσης και διαφάνειας. Η Google για παράδειγμα προσφέρει μια σελίδα πληροφοριών σχετικά με τη διαφήμιση και το απόρρητο[71]. Τα μέσα ενημέρωσης διαδραματίζουν πολύ σημαντικό ρόλο σε αυτόν τον τύπο εκπαίδευσης, συχνά με τη μορφή εκθέσεων παραβίασης απορρήτου από εταιρείες. Η σειρά «What They Know» της Wall Street Journal είναι το πιο γνωστό παράδειγμα[72]. Πρόσφατα, ακαδημαϊκοί ερευνητές έχουν γίνει πιο δραστήριοι στη μελέτη και την έκθεση παραβιάσεων απορρήτου και στην παρακολούθηση μέσω διαδικτύου.

Υπό το φως της παραπάνω συζήτησης, υπάρχει μια ποικιλία οντοτήτων που ενδιαφέρονται για την εκπαίδευση των καταναλωτών: κυβερνητικές υπηρεσίες, πολιτικές ελευθερίες και οργανώσεις υπεράσπισης καταναλωτών, τα μέσα ενημέρωσης, ακαδημαϊκοί, εταιρείες που εμπλέκονται στην online παρακολούθηση και προμηθευτές εργαλείων απορρήτου, συμπεριλαμβανομένων των προγραμμάτων περιήγησης στο Web. Δεν συμμετέχουν όλες οι οντότητες σε όλες τις κατηγορίες εκπαίδευσης, αλλά κάθε κατηγορία αντιπροσωπεύεται από πολλούς τύπους οργανισμών.

Ως τελική παρατήρηση αξίζει επίσης να σημειωθεί ότι πολλά πειραματικά αποτελέσματα στον τομέα της έρευνας για την προστασία της ιδιωτικής ζωής δείχνουν ότι τα πρωταρχικά ενδιαφέροντα για την πλειονότητα των χρηστών των διαδικτυακών υπηρεσιών είναι:

- η ευκολία χρήσης, και
- το κόστος υπηρεσίας (με προτίμηση για «δωρεάν» προσφορές)

Προφανώς και οι δύο αυτές προϋποθέσεις υποδηλώνουν την ανάγκη για τους χρήστες να δώσουν στους παρόχους υπηρεσιών προσωπικές πληροφορίες που δημιουργούν έσοδα από τους παρόχους σε αντάλλαγμα για τις «δωρεάν» υπηρεσίες που προσφέρονται.

# Κεφάλαιο 7

# Επίλογος

## 7.1 Συμπεράσματα - Συστάσεις

Ενώ υπάρχουν μερικά προστατευτικά μέτρα, όπως συζητήθηκε στην προηγούμενη ενότητα, η τρέχουσα κατάσταση δεν είναι ικανοποιητική από τη μεριά των καταναλωτών. Παραθέτουμε ορισμένα συμπεράσματα – ενδεικτικές προτάσεις, που απευθύνονται κυρίως σε ρυθμιστικές αρχές και τα οποία θα μπορούσαν να βοηθήσουν στη βελτίωση του απορρήτου των χρηστών.

Σε αυτήν την ενότητα λαμβάνεται επίσης υπόψη η δημοσίευση της ΕΕ για τη μεταρρύθμιση των κανόνων προστασίας δεδομένων [48].

### 7.1.1 Επικέντρωση στην παρακολούθηση, όχι στη Διαδικτυακή Συμπεριφορική Διαφήμιση (OBA)

Μεγάλο μέρος της συζήτησης σήμερα επικεντρώνεται στη Συμπεριφορική Διαφήμιση αντί της παρακολούθησης. Για παράδειγμα, ορισμένες διαφημιστικές εταιρείες ερμηνεύουν τη μη παρακολούθηση ως εξαίρεση των χρηστών από στοχευμένες διαφημίσεις συμπεριφοράς. Η παρακολούθηση εν γένει είναι το πρόβλημα, όχι η συμπεριφορική διαφήμιση. Η απαίτηση για μη παρακολούθηση πρέπει να ερμηνευθεί ως αίτημα για μη παρακολούθηση από τρίτους, είτε άμεσα είτε με τη βοήθεια του πρώτου μερούς.

### 7.1.2 Απόκτηση πιο ουσιαστικών πολιτικών απορρήτου

Παρόλο που το πρότυπο ειδοποίησης και επιλογής, που εφαρμόζεται συνήθως μέσω πολιτικών απορρήτου, παρουσιάζεται συχνά ως λύση για την προστασία της ιδιωτικής ζωής, έχει σοβαρούς περιορισμούς. Πρώτον, οι πολιτικές απορρήτου είναι συνήθως μακρές και περίπλοκες για να τις κατανοήσουν οι χρήστες και οι περισσότεροι απλώς τις αγνοούν. Δεύτερον, οι επιλογές του χρήστη είναι συνήθως δύο - είτε πρόκειται να αποδεχθεί την παρακολούθησή του για να χρησιμοποιήσει το προϊόν ή την υπηρεσία είτε να αρνηθεί και να αποχωρήσει από αυτή. Τέλος, πολλοί χρήστες δεν έχουν τις γνώσεις για να κατανοήσουν

πλήρως τις επιπτώσεις της συγκατάθεσης στην παρακολούθηση συμπεριφοράς ή την ευχέρεια, από τεχνική άποψη, να κάνουν τις επιθυμητές για αυτούς επιλογές.

Παρόλα αυτά τα προβλήματα, οι πολιτικές απορρήτου έχουν σημαντικό ρόλο να παίξουν κι αυτό γιατί αναγκάζουν τις εταιρείες να δεσμευτούν για τις πρακτικές που χρησιμοποιούν. Έχουν προταθεί αρκετές ιδέες για να καταστούν οι ειδοποιήσεις πιο σημαντικές και κατανοητές από τους καταναλωτές, όπως μια « ευκολονόητη ειδοποίηση» [50]. Οι ρυθμιστικές αρχές έχουν τρεις ρόλους: πρώτον, να διασφαλίσουν ότι οι εταιρείες καθορίζουν πολιτικές απορρήτου, δεύτερον, να ενθαρρύνουν τις εταιρείες να κάνουν αυτές τις πολιτικές ολοκληρωμένες, συγκεκριμένες και ουσιαστικές και τέλος, να διασφαλίζουν τη συμμόρφωση με τις δηλωμένες πολιτικές. Για παράδειγμα, το Υπουργείο Δικαιοσύνης της Καλιφόρνιας έχει θεσμοθετήσει μέτρα για να διασφαλίσει ότι όλες οι εφαρμογές για κινητά παρέχουν πολιτικές απορρήτου.

Μια πολύ σημαντική πτυχή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) όσο και της πρότασης για τον κανονισμό προστασίας της ιδιωτικής ζωής (ePrivacy Regulation) είναι η ενδυνάμωση των χρηστών κατά της εμπορικής και μη εκμετάλλευσης και της πιθανής κατάχρησης των δεδομένων τους. Από αυτή την άποψη, ο Κανονισμός είναι ένα κρίσιμο μέσο για την προστασία της ιδιωτικής ζωής. Η μετατροπή των νομοθετικών πράξεων από “οδηγίες” σε “κανονισμούς” τα τελευταία χρόνια, καθώς και η εισαγωγή οικονομικών επιπτώσεων, προστίμων και κυρώσεων στο πλαίσιο του νόμου αποτελούν τα πιο αποδοτικά κίνητρα για τη παρακίνηση της εξέλιξης του κλάδου της τεχνολογίας ως προς το σεβασμό των χρηστών. Ωστόσο, αν και το σαφές νομικό πλαίσιο είναι απαραίτητο, δεν αρκεί αν δεν συνοδεύεται από ανάπτυξη κατάλληλων τεχνολογιών που προάγουν την προστασία προσωπικών δεδομένων.

### 7.1.3 Ανάπτυξη εύχρηστων εργαλείων για διαφάνεια και έλεγχο

Όπως φαίνεται στο [51] οι περισσότεροι χρήστες δεν είναι εξοικειωμένοι με τη συμπεριφορική παρακολούθηση και διαφήμιση. Ένα μεγάλο μέρος των χρηστών δεν γνωρίζουν καν ότι παρακολουθούνται κι ότι δημιουργούνται τα προφίλ τους κατά την περιήγηση τους στον Ιστό και ότι τα προφίλ τους χρησιμοποιούνται για την προβολή στοχευμένων διαφημίσεων. Ενώ η περιοδική εκκαθάριση των cookies είναι ένα από τα απλούστερα μέτρα πρόληψης, μόνο μια μειονότητα χρηστών κατανοεί τι είναι ένα cookie, πώς χρησιμοποιούνται και πώς να τα

διαγράψουν. Οι χρήστες πρέπει να γνωρίζουν πώς χρησιμοποιούνται τα δεδομένα τους, σε τι επεξεργασία υποβάλλονται και ποιοι είναι οι πιθανοί κίνδυνοι. Υπάρχει ανάγκη ενισχυμένης διαφάνειας για να βοηθηθούν τα άτομα να κατανοήσουν πώς συλλέγονται, διαχειρίζονται και μεταφέρονται τα προσωπικά τους δεδομένα (και ιδανικά, οποιαδήποτε δεδομένα που μπορούν να χρησιμοποιηθούν σε μια επεξεργασία με πιθανά αποτελέσματα). Οι τεχνολογίες ιδιωτικότητας (PETs - Privacy Enhancing Technologies) είναι κρίσιμες δεδομένου ότι οι ροές πληροφοριών αυξάνονται δραματικά και οι τεχνικές εξόρυξης και εξαγωγής δεδομένων γίνονται όλο και πιο ισχυρές.

Μια πρωτοβουλία που πηγαίνει προς αυτή την κατεύθυνση είναι το πρόγραμμα βασισμένο σε εικονίδια που αναπτύχθηκε από μια ομάδα διαφημιστικών ενώσεων [52]. Αυτό το πρόγραμμα περιλαμβάνει τη χρήση ενός «Εικονιδίου Επιλογής Διαφήμισης», που οι έμποροι μπορούν να τοποθετήσουν κοντά στις διαφημίσεις τους ή στις ιστοσελίδες που συλλέγουν δεδομένα που χρησιμοποιούνται για στόχευση συμπεριφοράς. Οι χρήστες που κάνουν κλικ στο εικονίδιο βλέπουν μια εξήγηση για το γιατί βλέπουν μια συγκεκριμένη διαφήμιση και μπορούν να εξαιρεθούν από την παρακολούθηση. Δυστυχώς, αυτή η λύση δεν είναι πολύ καλή (τα εικονίδια είναι συχνά πολύ μικρά και δυσδιάκριτα και προκαλούν σύγχυση) [53]. Οι χρήστες δυσκολεύονται να κάνουν διάκριση μεταξύ των εταιρειών παρακολούθησης. Επιπλέον, ο κατάλογος των διαφημιστικών εταιρειών και οι τεχνολογίες παρακολούθησης αλλάζουν συνεχώς, καθιστώντας δύσκολο για τους παρόχους εργαλείων και τους χρήστες, να ελέγχουν τις κινήσεις τους στο διαδίκτυο.

Σε μια πιο αισιόδοξη σημείωση, διάφορες οντότητες όπως προμηθευτές προγραμμάτων περιήγησης, υποστηρικτές απορρήτου και ο Τύπος έχουν καταβάλει έντονες προσπάθειες για την ανάπτυξη πιο εύχρηστων εργαλείων διαφάνειας. Τα πρόσθετα Lightbeam 3.0 (γνωστό κατά τη φάση ανάπτυξης του ως Collusion Firefox της Mozilla) και Thunderbeam-Lightbeam για Chrome δείχνουν, σε πραγματικό χρόνο, όλα τα τρίτα μέρη που παρακολουθούν τον χρήστη σε ολόκληρο τον Ιστό. Το πρόσθετο Lightbeam δημιουργεί ένα δίκτυο αλληλεπιδράσεων μεταξύ εταιρειών και ιχνηλατών [49, 54]. Ωστόσο, απαιτείται πολύ περισσότερη χρηματοδότηση για να μπορεί να προχωρήσει η ανάπτυξη παρόμοιων εργαλείων.

Με βάση τα παραπάνω, ένα πιθανό πρώτο βήμα θα μπορούσε να είναι η Ευρωπαϊκή Επιτροπή (ενδεχομένως σε συνεργασία με ευρωπαϊκούς οργανισμούς όπως ο ENISA) να ξεκινήσει μια εκστρατεία ευαισθητοποίησης που θα ενημερώνει τους χρήστες πώς χρησιμοποιούνται / επεξεργάζονται τα δεδομένα τους και ποιοι είναι οι πιθανοί κίνδυνοι.

### 7.1.4 Ανάπτυξη πρωτοβουλιών συμμόρφωσης και παρακολούθησης

Θα πρέπει να προωθηθεί η αξιολόγηση επιπτώσεων απορρήτου και ενδεχομένως η πιστοποίηση απορρήτου. Διαδικασίες που προωθούν τη διαφάνεια και τη λογοδοσία μπορούν να συμβάλουν στην εμπιστοσύνη του κοινού στον τρόπο με τον οποίο η υπηρεσία ή η εφαρμογή διαχειρίζεται τα προσωπικά στοιχεία και παρακολουθεί τους χρήστες.

Οι λύσεις εξαίρεσης ή βάσει ειδοποιήσεων είναι αποτελεσματικές μόνο εάν οι εταιρείες ακολουθούν τους κανόνες και σέβονται τα αιτήματα των χρηστών να μην παρακολουθούνται, καθώς και να τηρούν τις υποσχέσεις τους. Ενώ οι περισσότερες εταιρίες συμμορφώνονται με τα πρότυπα αυτορρύθμισης, έχει αποδειχθεί ότι πολλές μικρότερες εταιρείες δεν το κάνουν αυτό [55].

Οι υπηρεσίες και οι εφαρμογές θα πρέπει επομένως να ελέγχονται για διαρροή / παρακολούθηση δεδομένων και τα αποτελέσματα θα πρέπει να δημοσιοποιούνται. Τα μέσα ενημέρωσης διαδραματίζουν πολύ σημαντικό ρόλο σε αυτή τη διάδοση πληροφοριών. Είναι σημαντικό να σημειωθεί ότι επειδή ενδέχεται να επιτρέπονται ορισμένοι τύποι παρακολούθησης, τα εν λόγω εργαλεία είναι απλώς βοηθήματα για να προσδιορίσουν πότε απαιτείται περαιτέρω έρευνα.

Θα πρέπει να αναπτυχθούν λύσεις για τον αποκλεισμό εταιριών που έχουν αποδεδειγμένα κακή συμπεριφορά ή να γίνει προσπάθεια μέσω της νομικής οδού να συμμορφωθούν με τους κανόνες και τη νομοθεσία. Ένα δύσκολο ζήτημα για τους οργανισμούς επιβολής είναι το ζήτημα των υπεράκτιων εταιρειών παρακολούθησης. Μια προτεινόμενη λύση είναι να απαγορεύεται στα πρώτα μέρη να συνεργάζονται με τρίτα μέρη που δεν συμμορφώνονται.

Το Ευρωπαϊκό Κέντρο Ψηφιακών Δικαιωμάτων (NOYB) [95] είναι ένας μη κερδοσκοπικός οργανισμός που εδρεύει στη Βιέννη της Αυστρίας και ιδρύθηκε το 2017. Η NOYB χρησιμοποιεί βέλτιστες πρακτικές από ομάδες δικαιωμάτων των καταναλωτών, ακτιβιστές για την προστασία της ιδιωτικής ζωής, χάκερς και νομικές τεχνολογικές πρωτοβουλίες και τις

συγχωνεύει σε μια Ευρωπαϊκή πλατφόρμα εφαρμογής του νόμου. Μαζί με τις πολλές νέες δυνατότητες εφαρμογής του νόμου σύμφωνα με τον κανονισμό της ΕΕ για την προστασία των δεδομένων (GDPR) και του υπό έγκριση κανονισμού ePrivacy, η NOYB μπορεί να υποστηρίζει υποθέσεις προστασίας της ιδιωτικής ζωής με πολύ πιο αποτελεσματικό τρόπο από πριν. Επιπλέον, η NOYB ακολουθεί την ιδέα της στοχευμένης και στρατηγικής νομικής διαμάχης, προκειμένου να ενισχύσει το δικαίωμά των χρηστών στην ιδιωτική ζωή.

Ο GDPR προσπαθεί να διασφαλίσει ότι οι χρήστες θα έχουν πλήρη έλεγχο των δεδομένων τους, αλλά η πλοήγηση στο διαδίκτυο έχει γίνει μια περίπλοκη και απογοητευτική εμπειρία για τους ανθρώπους σε όλη την Ευρώπη. Ενοχλητικά cookie banners εμφανίζονται σε κάθε γωνιά του διαδικτύου, καθιστώντας συχνά εξαιρετικά περίπλοκο για τους χρήστες να πατήσουν οτιδήποτε άλλο εκτός από το κουμπί "αποδοχή" – κάτι που βεβαίως δεν συνιστά ελεύθερη συγκατάθεσή τους. Οι εταιρείες χρησιμοποιούν τα λεγόμενα "σκοτεινά μοτίβα" (dark patterns) για να πείσουν πάνω από το 90% των χρηστών να "συμφωνήσουν", όταν οι στατιστικές της βιομηχανίας δείχνουν ότι μόνο το 3% των χρηστών θέλει πραγματικά να συμφωνήσει. Σε μια παρόμοια έρευνα σχετικά με την αληθινή συγκατάθεση των χρηστών, η Apple προχώρησε στον εκ νέου σχεδιασμό ενημέρωσης των χρηστών προσφέροντας μια σαφή επιλογή για τους χρήστες όταν το Apple Advertisement ID κοινοποιείται σε μια εφαρμογή. Αυτή η ουδέτερη σχεδίαση οδηγεί σε περισσότερο από το 90% όλων των χρηστών των ΗΠΑ να αρνούνται την παρακολούθηση [97] .

Σύμφωνα με το νόμο, πρέπει να δίνεται στους χρήστες μια σαφής και ελεύθερη επιλογή "ναι/όχι" για τη χρήση cookies για σκοπούς διαφήμισης. Καθώς τα περισσότερα banners δεν συμμορφώνονται με τις απαιτήσεις του GDPR, η NOYB ανέπτυξε ένα λογισμικό που αναγνωρίζει τους διάφορους τύπους παράνομων cookie banners και δημιουργεί αυτόματα τις σχετικές καταγγελίες. Η NOYB δίνει ωστόσο στις εταιρείες μια περίοδο χάριτος ενός μηνός για να συμμορφωθούν με τους νόμους της ΕΕ πριν από την υποβολή της επίσημης καταγγελίας. Η NOYB σκοπεύει να χρησιμοποιήσει αυτό το σύστημα για να εξασφαλίσει τη συμμόρφωση έως και 10.000 από τους πιο επισκέψιμους ιστότοπους στην Ευρώπη κατά τη διάρκεια ενός έτους. Εάν το πετύχει, οι χρήστες θα πρέπει να δουν απλές και σαφείς επιλογές "ναι ή όχι" σε όλο και περισσότερους ιστότοπους τους επόμενους μήνες.

Πολύ πρόσφατα, μόλις τον Μάϊο του 2021 το νέο αυτό σύστημα παρέδωσε τα πρώτα σχέδια καταγγελιών σε 560 ιστότοπους από 33 χώρες, συμπεριλαμβανομένων όλων των κρατών μελών της ΕΕ/ΕΟΧ εκτός από τη Μάλτα και το Λιχτενστάιν.

Η Γαλλική Αρχή Προστασίας Δεδομένων CNIL (Commission nationale de l'informatique et des libertés/ National Commission on Informatics and Liberty) εξέδωσε πρόσφατα οδηγίες σχετικά με τα cookie banners και επίσης ανακοίνωσε τις πρώτες ενέργειες επιβολής των ευρωπαϊκού κανονισμού για την προστασία των δεδομένων. Οι ενέργειες της CNIL είναι πολύ κοντά σε αυτές του NOYB.

### 7.1.5 Ανάπτυξη πρωτοβουλιών κατά της παρακολούθησης για εφαρμογές για κινητά

Η παρακολούθηση τρίτων πολλαπλασιάζεται σε πλατφόρμες για κινητά [16]. Ωστόσο, οι τρέχουσες λύσεις που βασίζονται σε προγράμματα περιήγησης, δεν έχουν ακόμη προσαρμοστεί αποτελεσματικά σε πλατφόρμες για κινητά - μεγάλο μέρος της παρακολούθησης τρίτων σε κινητές συσκευές συμβαίνει σε εφαρμογές για κινητά, εκτός του πλαισίου ενός παραδοσιακού προγράμματος περιήγησης. Οι μηχανισμοί παρακολούθησης συχνά ενσωματώνονται σε εφαρμογές, ή μάλλον στις διαφημιστικές βιβλιοθήκες που χρησιμοποιούν [74]. Κατά συνέπεια, δεν υπάρχει τρόπος να εκφράσει ο χρήστης ότι δεν θέλει να παρακολουθείται χωρίς να απεγκαταστήσει τις εφαρμογές. Πρέπει να αναπτυχθούν λύσεις προσαρμοσμένες σε πλατφόρμες για κινητά.

### 7.1.6 Προώθηση του απορρήτου-μέσω-σχεδιασμού

Αν και έχουν προταθεί μερικές εναλλακτικές λύσεις για την προστασία της ιδιωτικής ζωής στην παρακολούθηση, αυτές οι λύσεις έχουν υιοθετηθεί ελάχιστα ή καθόλου. Από την άποψη των διαφημιστικών εταιρειών, των κοινωνικών δικτύων κι άλλων εταιρειών που συλλέγουν δεδομένα, οι λύσεις διατήρησης της ιδιωτικής ζωής έρχονται με πιθανώς κόστος απόδοσης, χωρίς άμεσο όφελος. Η πίεση από τους υπερασπιστές της ιδιωτικής ζωής έχει αποδειχθεί μέχρι στιγμής αρκετά ανεπαρκής. Οι Κανονισμοί έχουν σημαντικό ρόλο να διαδραματίσουν, ώστε να δημιουργηθούν τα αντίστοιχα κίνητρα στις εταιρείες να υιοθετήσουν λύσεις διατήρησης της ιδιωτικής ζωής. Γενικότερα, το βάρος της επιβολής του διαδικτυακού απορρήτου πρέπει να μεταφερθεί στις επιχειρήσεις. Αυτό θα ωθήσει τις εταιρείες να ενσωματώσουν το απόρρητο στα προϊόντα και τις διαδικασίες τους ήδη εκ της σχεδίασής του (privacy by design), αντί να

αποποιούνται των ευθυνών τους για την προστασία της ιδιωτικότητας και το απόρρητο μέσω της απλής υιοθέτησης δυσνόητων μακροσκελών και πολλές φορές παραπλανητικών νομικών ειδοποιήσεων.

### 7.1.7 Ενίσχυση του νομικού πλαισίου

Αν και, όπως αναφέρθηκε, ένα σαφές και ορθό νομικό πλαίσιο από μόνο του δεν μπορεί να είναι αρκετό, εν τούτοις είναι απόλυτα απαραίτητο. Σε αυτό το πλαίσιο, είναι σημαντικό να υπάρξουν κατάλληλες προβλέψεις στον υπό διαμόρφωση e-Privacy Κανονισμό της Ευρωπαϊκής Ένωσης. Μία σημαντική πτυχή είναι το γεγονός ότι θα πρέπει να προβλέπονται συγκεκριμένες υποχρεώσεις και για όσους αναπτύσσουν εφαρμογές ή προϊόντα (applications and product developers) τα οποία διαθέτουν σε οργανισμούς, αφού οι εν λόγω φορείς μέχρι τώρα, λόγω του ότι δεν επεξεργάζονται οι ίδιοι προσωπικά δεδομένα αλλά παρέχουν εργαλεία που χρησιμοποιούνται για το σκοπό αυτό, εξαιρούνται από ένα σύνολο υποχρεώσεων που διέπει τους οργανισμούς που επεξεργάζονται δεδομένα: αν όμως τα τεχνολογικά εργαλεία δεν είναι σχεδιασμένα κατάλληλα, η συμμόρφωση των οργανισμών καθίσταται δυστυχώς δύσκολη εξ αρχής.

# Βιβλιογραφία


[1] Omer Tene and Jules Polonetsky, 'To Track or "Do Not Track": Advancing transparency and individual control in online behavioral Advertising', Minnesota Journal of Law, Science & Technology, Volume 13, Issue 1, Winter 2012.

[2] Raphael, J. R., 'Apple vs. Android location tracking: Time for some truth', https://www.computerworld.com/article/2471210/apple-vs--android-location-tracking--time-for-some-truth.html

[3] Google Analytics, Enterprise-class web analytics, https://marketingplatform.google.com/about/analytics-360/

[4] Peter Eckerley, 'How Online Tracking Companies Know Most of What You Do Online', https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks

[5] Schoen, S., 'New Cookie Technologies: Harder to See and Remove, Widely Used to Track You', https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide

[6] A Guide for Consumers Who Want to Protect Their Privacy and Companies That Want to Respect Consumer Choice, https://www.eff.org/pages/understanding-effs-do-not-track-policy-universal-opt-out-tracking

[7] Bujlow et al., 2015 'Web Tracking: Mechanisms, Implications and Defenses, https://www.researchgate.net/publication/280590332_Web_Tracking_Mechanisms_Implications_and_Defenses

[8] Ashkan, S., S. Canty, M. Quentin, T. Lauren, and J. Chris, 'Flash cookies and privacy. Technical report', University of California, Berkeley, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

[9] Kamkar, S. (October 2010). 'Evercookie – never forget' https://samy.pl/evercookie/

[10] Eckersley, P.: 'How unique is your web browser?' In: Atallah, M.J., Hopper, N.J.(eds.) PETS 2010. LNCS, vol. 6205, pp. 1–18. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14527-8_1

[11] Krishnamurthy, B. and C. Wills, 'Privacy diffusion on the web: a longitudinal perspective', in WWW '09: Proceedings of the 18th international conference on World wide web. ACM. https://dl.acm.org/doi/10.1145/1526709.1526782

[12] Newman, Lily Hay (12 October 2018). 'A New Google+ Blunder Exposed Data From 52.5 Million Users'. Wired. ISSN 1059-1028 https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/

[13] Krishnamurthy, B. and C. Wills, 'On the leakage of personally identifiable information via online social networks', in WOSN '09: The second workshop on Online social networks.

[14] A. Chaabane, G. Acs, M. A. Kaafar, 'You Are What You Like! Information leakage through users' Interests', The Network & Distributed System Security Symposium (NDSS), San Diego, 2012.

[15] A. Chaabane, M. A. Kaafar, R. Borelli, 'Big Friend is Watching You: Analyzing online social networks tracking capabilities', in Workshop on Online Social Networks (WOSN'12), Helsinki, 2012.

[16] S. Thurm and Y. Kane, 'Your Apps Are Watching You', The Wall Street Journal, Dec. 2010. https://www.wsj.com/articles/SB10001424052748704694004576020083703574602

[17] A. Narayanan. 'There is no such thing as anonymous online tracking', available at: http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking

[18] Balachander Krishnamurthy, Konstantin Naryshkin and Craig Wills, 'Privacy leakage vs. Protection measures: the growing disconnect', Web 2.0 Security and Privacy Workshop, May 2011.

[19] Arvind Narayanan, Vitaly Shmatikov. 'Robust de-anonymization of large sparse datasets', IEEE S&P '08.

[20] Daniele Perito, Claude Castelluccia, Mohamed Ali Kaafar, Pere Manils. 'How Unique and Traceable are Usernames?', 11th Privacy Enhancing Technologies Symposium (PETS 2011), Waterloo, CA, 2011.

[21] Arvind Narayan, 'The Linkability of Usernames: a Step Toward "Uber-profiles"', blog posts, Feb. 2011. https://33bits.wordpress.com/2011/02/16/usernames-linkability-uber-profiles/

[22] Greene, K. (August 1, 2014) 'Reality mining', MIT Tech. https://mitpress.mit.edu/books/reality-mining

[23] Boulton, C., 'Google CEO Schmidt Pitches Autonomous Search, Flirts with AI', https://www.eweek.com/news/google-ceo-schmidt-pitches-autonomous-search-flirts-with-ai/

[24] A. Acquisti, R. Gross and F. Stutzman, 'Faces of Facebook: Privacy in the Age of Augmented Reality', BlackHat Las Vegas, August 4, 2011 https://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/

[25] C. Duhigg, 'How Companies Learn Your Secrets', The New York Times, February 2012, available at: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all

[26] Solove, Daniel J., 'Nothing to Hide: The False Tradeoff between Privacy and Security', May 1, 2011. GWU Law School Public Law Research Paper No. 571.

[27] Arvind Narayanan, 'Price Discrimination is All Around You', https://33bits.wordpress.com/2011/06/02/price-discrimination-is-all-around-you/

[28] Eli Pariser, 'The Filter Bubble: What the Internet is Hiding from You', Penguin Press, March 2011.

[29] C. Castelluccia, E. De Cristofaro, and D. Perito, 'Private information disclosure from web searches', in Proceedings of the 2010 Privacy Enhancing Technologies Symposium (PETS), Berlin, Germany, 2010.

[30] Castelluccia, C., D. Kaafar and D.M Tran, 'Betrayed by Your Ads', in Proceedings of the 2012 Privacy Enhancing Technologies Symposium (PETS), Vigo, Spain, 2012.

[31] NoScript Firefox extension, 2021, https://noscript.net/

[32] G. Aggrawal, E. Bursztein, C. Jackson, and D. Boneh, 'An analysis of private browsing modes in modern browsers', in Proceedings of 19th Usenix Security Symposium, 2010.

[33] R. Dingledine, N. Mathewson, and P. Syverson. 'Tor: The second-generation onion router', in Usenix security symposium, 2004.

[34] Do Not Track-Universal Tracking Opt Out, https://www.eff.org/issues/do-not-track

[35] S. Guha, B. Cheng and P. Francis. 'Privad: Practical Privacy in Online Advertising', in Proceedings of the 8th Symposium on Networked Systems Design and Implementation (NSDI), Boston, MA, Mar 2011.

[36] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, and Solon Barocas, 'Adnostic: Privacy preserving targeted advertising', NDSS, San Diego, USA, 2010.

[37] Matthew Fredrikson and Benjamin Livshits. 'RePriv: Re-envisioning in-browser privacy', in IEEE Symposium on Security and Privacy, May 2011.

[38] Article 29 Data Protection Working Party, (2011, August) Letter to the online advertising industry (OBA) Industry regarding the self-regulatory Framework, available at: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf

[39] Article 29 Data Protection Working Party, (2010, June) Opinion 2/2010 on online behavioural advertising, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[40] European Commission, 'Commission proposes a comprehensive reform of the data protection rules' https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

[41] J. Mullen, 'Judge approves $2.4 million Quantcast privacy settlement' https://gigaom.com/2011/06/14/419-judge-approves-2-4-million-quantcast-privacy-settlement/

[42], 'Second privacy law suit over cookies' falls apart' https://gigaom.com/2011/08/18/419-privacy-lawsuits-over-flash-cookies-falling-apart/

[43] Announcement of Formal Withdrawal of The "IAB Europe OBA Framework" of 2011 https://iabeurope.eu/all-news/announcement-of-formal-withdrawal-of-the-iab-europe-oba-framework-of-2011/

[44] Digital Advertising Alliance, 'Self-regulatory principles for multi-site data', November 2011, https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Multi-Site-Data-Principles.pdf

[45] R. Gellman and P. Dixon, 'Many failures: A brief history of privacy self-regulation in the United States', October 2011, http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf

[46] Tracking Protection Working Group. W3C. https://www.w3.org/2011/tracking-protection/

[47] R. Tirtea, C. Castelluccia and D. Ikonomou (ENISA), 'Bittersweet cookies. Some security and privacy considerations', https://www.enisa.europa.eu/publications/copy_of_cookies/at_download/fullReport

[48] Μεταρρύθμιση των κανόνων προστασίας δεδομένων της ΕΕ, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_el

[49] Thunderbeam-Lightbeam for Chrome https://chrome.google.com/webstore/detail/thunderbeam-lightbeam-for/hjkajeglckopdkbggdiajobpilgccgnj?hl=en-GB

[50] R. Calo, 'Against Notice Skepticism', Notre Dame Law Review 1027, 2012.

[51] McDonald, A. M., and Cranor, L. F. 'Americans' Attitudes about Internet Behavioral Advertising Practices', Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES) October 4, 2010.

[52] Advertising Option Icon program, 2012, https://www.wordstream.com/blog/ws/2014/01/22/adchoices

[53] Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang, 'Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising', CMU technical report CMU-CyLab-11-017, October 31, 2011.

[54] Mozilla LightBeam add-on, https://addons.mozilla.org/el/firefox/addon/lightbeam-3-0/

[55] Saranga Komanduri, Richard Shay, Greg Norcie, Blase Ur, Lorrie Faith Cranor, 'AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements', CMU TR CMU-CyLab-11-005, March 2011.

[56] Rebecca Balebako, Pedro Leon, Richard Shay, Blase U, and Lorrie Cranor, 'Measuring the Effectiveness of Privacy Tools for Limiting Behavioral Advertising', Web 2.0 Security and Privacy Conference 2012.

[57] ENISA Privacy considerations of online behavioural tracking, November 2012, https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking

[58] Ting-Fang Yen, Yinglian Xie, Fang Yu, Roger P. Yu, Martin Abadi, 'Host Fingerprinting and Tracking on the Web: Privacy and Security Implications', in Proceedings of the 19th Annual Network & Distributed System Security Symposium (February 2012)

[59] Federal Trade Commission (2011, March) 'FTC puts an end to tactics of online advertising company that deceived consumers who wanted to 'opt out' from targeted ads', https://www.ftc.gov/news-events/press-releases/2011/03/ftc-puts-end-tactics-online-advertising-company-deceived

[60] Federal Trade Commission (2011, November) 'Online advertiser settles FTC charges ScanScout deceptively used Flash cookies to track consumers online', https://www.ftc.gov/news-events/press-releases/2011/11/online-advertiser-settles-ftc-charges-scanscout-deceptively-used

[61] The Privacy Sandbox - The Chromium Projects, https://www.chromium.org/Home/chromium-privacy/privacy-sandbox

[62] Adobe Flash Player EOL Enterprise Information Page, https://www.adobe.com/products/flashplayer/enterprise-end-of-life.html

[63] Have you had enough of cookie banners? Forget about them! Ninja Cookie will take care of these and can say "no" to them for you!, https://ninja-cookie.com/

[64] ENISA's PETs Maturity Assessment Repository, January 2019, https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository/at_download/fullReport

[65] Data protection - Rules for the protection of personal data inside and outside the EU, https://ec.europa.eu/info/law/law-topic/data-protection_en

[66] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EL

[67] California Consumer Privacy Act (CCPA), 2018, https://oag.ca.gov/privacy/ccpa

[68] Global Privacy Control (GPC), https://globalprivacycontrol.org/

[69] CDT's Guide to Behavioral Advertising, October 27, 2009, https://cdt.org/insights/cdts-guide-to-behavioral-advertising/

[70] EFF's Top 12 Ways to Protect Your Online Privacy, APRIL 9, 2002, https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy

[71] Creating a safer and better internet for children and young people
, https://www.betterinternetforkids.eu/

[72] ΔΙΑΦΗΜΙΣΕΙΣ, https://policies.google.com/technologies/ads

[73] What They Know - The Business of Tracking You on the Internet, A Wall Street Journal Investigation, http://www.cs.cornell.edu/~shmat/courses/cs5436/whattheyknow.pdf

[74] Michael Grace et al., 'Unsafe Exposure Analysis of Mobile In-App Advertisements', ACM Wisec 2012.

[75] Bujlow, T., Carela-Español, V., Solé-Pareta, J., Barlet-Ros, P.: A survey on web tracking: mechanisms, implications,and defenses. Proc. IEEE 105,1476–1510(2017), https://doi.org/10.1109/jproc.2016.2637878

[76] Castelluccia, C.: 'Behavioural tracking on the internet: a technical perspective.' In: Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (eds.) European Data Protection: In Good Health, pp. 21–33. Springer, Heidelberg (2012). https://doi.org/10.1007/978-94-007-2903-2_2

[77] Kurtz, A., Gascon, H., Becker, T., Rieck, K., Freiling. F.: Fingerprinting mobile devices using personalized configurations. In: Proceedings on Privacy Enhancing Technologies (PoPETs), vol. 1, pp. 4–19 (2016). https://doi.org/10.1515/popets-2015-0027

[78] Krumm, J.: Ubiquitous advertising: the killer application for the 21st century. IEEE Pervasive Comput. 10, 66–73 (2010), https://doi.org/10.1109/mprv.2010.21

[79] Castelluccia, C.: Behavioural tracking on the internet: a technical perspective. In: Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (eds.) European Data Protection: In Good Health, pp. 21–33. Springer, Heidelberg (2012), https://doi.org/10.1007/978-94-007-2903-2_2

[80] Athanasopoulos, E., Kemerlis, V.P., Portokalidis, G., Keromytis, A.D.: NaClDroid: native code isolation for android applications. In: Askoxylakis, I., Ioannidis, S., Katsikas, S., Meadows, C. (eds.) ESORICS 2016. LNCS, vol. 9878, pp. 422–439, Springer, Cham (2016), https://doi.org/10.1007/978-3-319-45744-4_21

[81] Taylor, V.F., Beresford, A.R., Martinovic, I.: Intra-Library Collusion: A Potential Privacy Nightmare on Smartphones. arXiv:1708.03520v1 [cs.CR] (2017)

[82] Ikram, M., Kaafar, M. A.: A first look at mobile Ad-Blocking apps. In IEEE 16th International Symposium on Network Computing and Applications (NCA), pp.1–8 (2017), https://doi.org/10.1109/NCA.2017.8171376

[83] Gervais, A., Filios, A., Lenders, V., Capkun, S.: Quantifying web adblocker privacy. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) ESORICS 2017. LNCS, vol. 10493, pp. 21–42. Springer, Cham (2017), https://doi.org/10.1007/978-3-319-66399-9_2

[84] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., Shadbolt, N.: Third Party Tracking in the Mobile Ecosystem. arXiv:1804.03603v3 [cs.CY] (2018)

[85] Stevens, R., Gibler, C., Crussell, J., Erickson, J., Chen, H.: Investigating user privacy in Android ad libraries. In: Workshop on Mobile Security Technologies (MoST), p. 10 (2012)

[86] GSM Association: Safety, privacy and security across the mobile ecosystem - Key issues and policy implications, 2017 https://www.gsma.com/publicpolicy/wpcontent/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobileecosystem.pdf

[87] Pavlou, P., & Stewart, D. (2015). Interactive advertising: A new conceptual framework towards integrating elements of the marketing mix. In M. Moore & R. S.Moore (Eds.), New Meanings for Marketing in a New Millennium (pp. 218-222), Springer International Publishing

[88] Gray, C. H. (2014). Who pays the price?: Regulation of data tracking & online behavioral advertising. SSRN: http://ssrn.com/abstract=2556525

[89] Nancy J.KingV.T.Raja (2012), Protecting the privacy and security of sensitive customer data in the cloud, https://doi.org/10.1016/j.clsr.2012.03.003

[90] Ho, S. Y. (2006). The attraction of internet personalization to web users. Electronic Markets, 16(1), 41-50, doi:10.1080/10196780500491162

[91] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

[92] S. Yuan, J. Wang, X. Zhao, 'Real-time Bidding for Online Advertising: Measurement and Analysis', https://arxiv.org/abs/1306.6542

[93] Chan, Rosalie. 'The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections'. Business Insider,2020, https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10

[94] N. Nikiforakis, A. K. (2013). Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting,. 2013 IEEE Symposium on Security and Privacy, 541-555

[95] My Privacy is None of Your Business, 2021 https://noyb.eu/en

[96] 'Panopticlick - A Project of the Electronic Frontier Foundation', https://coveryourtracks.eff.org/

[97] 'iOS 14.5 Opt-in Rate - Daily Updates Since Launch', Estelle Laziuk, Flurry Analyst https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/

[98] Ting-Fang Yen, Yinglian Xie, Fang Yu, Roger P. Yu, Martin Abadi, 'Host Fingerprinting and Tracking on the Web: Privacy and Security Implications', in Proceedings of the 19th Annual Network & Distributed System Security Symposium (February 2012).